This is a digital copy of a book that was preserved for generations on library shelves before it was carefully scanned by Google as part of a project to make the world's books discoverable online.

It has survived long enough for the copyright to expire and the book to enter the public domain. A public domain book is one that was never subject to copyright or whose legal copyright term has expired. Whether a book is in the public domain may vary country to country. Public domain books are our gateways to the past, representing a wealth of history, culture and knowledge that's often difficult to discover.

Marks, notations and other marginalia present in the original volume will appear in this file - a reminder of this book's long journey from the publisher to a library and finally to you.

Usage guidelines

Google is proud to partner with libraries to digitize public domain materials and make them widely accessible. Public domain books belong to the public and we are merely their custodians. Nevertheless, this work is expensive, so in order to keep providing this resource, we have taken steps to prevent abuse by commercial parties, including placing technical restrictions on automated querying.

We also ask that you:

+ *Make non-commercial use of the files* We designed Google Book Search for use by individuals, and we request that you use these files for personal, non-commercial purposes.

+ *Refrain from automated querying* Do not send automated queries of any sort to Google's system: If you are conducting research on machine translation, optical character recognition or other areas where access to a large amount of text is helpful, please contact us. We encourage the use of public domain materials for these purposes and may be able to help.

+ *Maintain attribution* The Google "watermark" you see on each file is essential for informing people about this project and helping them find additional materials through Google Book Search. Please do not remove it.

+ *Keep it legal* Whatever your use, remember that you are responsible for ensuring that what you are doing is legal. Do not assume that just because we believe a book is in the public domain for users in the United States, that the work is also in the public domain for users in other countries. Whether a book is still in copyright varies from country to country, and we can't offer guidance on whether any specific use of any specific book is allowed. Please do not assume that a book's appearance in Google Book Search means it can be used in any manner anywhere in the world. Copyright infringement liability can be quite severe.

About Google Book Search

Google's mission is to organize the world's information and to make it universally accessible and useful. Google Book Search helps readers discover the world's books while helping authors and publishers reach new audiences. You can search through the full text of this book on the web at `http://books.google.com/`

Stanford University Libraries
3 6105 001 014 997

610.6
L847

PROCEEDINGS

OF

THE LONDON MATHEMATICAL SOCIETY.

VOL. XXXIII.

NOVEMBER, 1900, TO FEBRUARY, 1901.

LONDON:
FRANCIS HODGSON, 89 FARRINGDON STREET, E.C.

1901.

LONDON:
PRINTED BY C. F. HODGSON & SON,
2 NEWTON STREET, HIGH HOLBORN, W.C.

LIBRARY
Leland Stanford, Jr.
UNIVERSITY

a. 61303

PROCEEDINGS

OF

THE LONDON MATHEMATICAL SOCIETY.

VOL. XXXIII.

THIRTY-SEVENTH SESSION, 1900–1901

(since the Formation of the Society, January 16th, 1865).

November 8th, 1900.

THE SEVENTH ANNUAL GENERAL MEETING OF THE LONDON MATHEMATICAL SOCIETY, as incorporated under the Companies Act, 1867, on October 23rd, 1894, held at 22 Albemarle Street, W.

Lord KELVIN, G.C.V.O., President, in the Chair.

Twenty-four members present.

The Treasurer read his report, the reception of which was moved by Mr. Kempe, seconded by Mr. W. F. Sheppard, and carried unanimously.

The President said, if it was the pleasure of the meeting, Mr. Gallop would be asked again to act as Auditor. Carried unanimously.

The senior Secretary announced that there had been three deaths, of which he had received intimation, during the session, viz., of Prof. Beltrami (an honorary member), Mr. J. J. Walker, and Major-General Close, R.A.

There had been no addition to the list of exchanges.

The following societies and persons, not members of the Society, receive the *Proceedings of the London Mathematical Society*, in exchange for their own *Proceedings*, or for some other reason :—

1. The Royal Society.
2. The Royal Society of Edinburgh.
3. The Royal Irish Academy.
4. The Library of Trinity College, *Dublin.*
5. The Cambridge Philosophical Society.
6. The Philosophical Society of Manchester.
7. The Institute of Actuaries.
8. The Library of University College, *Gower Street.*
9. The Superintendent, Copyright Office of the British Museum.
10. The University Library, *Cambridge.*
11. The Bodleian Library, *Oxford.*
12. The Faculty of Advocates' Library, *Edinburgh.*
13. The Mason Science College Library, *Birmingham.*
14. The Edinburgh Mathematical Society, *Edinburgh.*
15. The Editor of *Nature.*
16. The Canadian Institute, *Toronto.*
17. The Smithsonian Institute, *Washington, D.C., U.S.A.*
18. The United States Naval Observatory, *Washington, D.C., U.S.A.*
19. The Connecticut Academy, *Newhaven, Conn., U.S.A.*
20. The Editors of the "American Journal of Mathematics," *Johns Hopkins University, Baltimore, U.S.A.*
21. The Editors of "The Annals of Mathematics," 2 *University Hall, Cambridge, Mass., U.S.A.*
22. L'Institut National de France, *Paris.*
23. La Société Mathématique, 7 *Rue des Grands Augustins, Paris.*
24. La Société Philomathique, 7 *Rue des Grands Augustins, Paris.*
25. M. le Général commandant l'Ecole Polytechnique, *Paris.*
26. La Société des Sciences Physiques et Naturelles, *Bordeaux.*
27. La Bibliothèque Universitaire de Médecin et des Sciences alliées, *St. Michel, Toulouse.*
28. L'Académie Royale des Sciences, des Lettres et des Beaux Arts de Belgique, *Palais des Académies, Bruxelles.*
29. La Société Hollandaise (par l'entremise du Bureau Scientifique Central Néerlandais), *Haarlem.*
30. The Editors of the "Annales de l'Ecole Polytechnique à Delft," *Delft.*
31. The Mathematical Society of Amsterdam.
32. Reale Istituto Lombardo di Scienze e Lettere, *Milan.*
33. Reale Accademia dei Lincei, *Palazzo delle Scienze, Lungara* 10, *Roma.*
34. Reale Accademia di Scienze, Lettere ed Arti, *Modena.*
35. Reale Accademia delle Scienze fisiche e matematiche, *Napoli.*
36. Reale Istituto Veneto di Scienze, Lettere ed Arti, *Venezia.*
37. Circolo Matematico di Palermo.
38. M. le Prof. Gomes Teixeira, *Coimbra.*
39. La Société Mathématique (Cabinet de Mécanique, Université), *Odessa.*
40. Akademie der Wissenschaften, *Berlin.*

41. The Editor of the "Journal für die reine und angewandte Mathematik (*Crelle*)," *Berlin.*

42. The Authors of the "Jahrbuch über die Fortschritte der Mathematik," *Berlin.*

43. Die Königliche Gesellschaft der Wissenschaften, *Göttingen.*

44. The Librarian (an der Physischen und Medicinischen Gesellschaft), *Erlangen.*

45. The Editor of the "Beiblätter zu den Annalen der Physik und Chemie," *Leipzig.*

46. Die Königliche Sächsische Gesellschaft, *Leipzig.*

47. Die Naturforschende Gesellschaft, *Zurich.*

48. The Editors of the "Prace-Matematyczno Fizyczne" of *Warsaw.*

49. Le Rédacteur de "Nieuw Archiev," *Leiden.*

50. La Faculté des Sciences de Marseille.

51. The Physical Society, *London.*

52. The Editor of the "Monatshefte für Mathematik und Physik," *Vienna.*

53. The American Mathematical Society, *New York.*

54. The American Philosophical Society, *Philadelphia*

55. The Editor of the "Periodico di Matematica per l'insegnamento secondario."

56. University College of North Wales, Bangor.

Extra work had been undertaken by the Secretaries in the form of a *Complete Index of all the Papers printed in the Proceedings of the London Mathematical Society, Vols. I.–XXX.* (112 pp.); and of a *List of Members of the London Mathematical Society, from the date of foundation,* 16*th January,* 1865, *to* 9*th November,* 1899 (16 pp.).

Mr. Love reported that at the beginning of the Session the number of members was 247, deaths had been 2, name restored 1, and new members 6, making a total of members, at the commencement of the new Session, equal 252. In addition, the Society had to regret the loss of one foreign member.

Messrs. M. Jenkins and W. W. Taylor having consented to act as Scrutineers, the ballot was then taken, with the result that the gentlemen who had been nominated by the Council were declared by the President to have been elected to constitute the Council for the Session 1900–1901. Their names are:—President, Dr. Hobson; Vice-Presidents, Lord Kelvin, Prof. W. Burnside, and Major P. A. MacMahon; Treasurer, Dr. J. Larmor; Hon. Secs., Mr. R. Tucker and Prof. Love. Other members: Mr. J. E. Campbell, Lt.-Col. Cunningham, Prof. Elliott, Dr. Glaisher, Prof. M. J. M. Hill, Mr. Kempe, Mr. H. M. Macdonald, Mr. A. E. Western, and Mr. E. T. Whittaker.

Lord Kelvin on leaving the Chair thanked the Society for their having elected him to the office of President, and for their tolerating so kindly his infrequent attendance at their meetings—"a result due to the interval of four hundred miles which lay between his home and London." He then welcomed Dr. Hobson to the vacant Chair, and expressed his "pleasure in having him for his successor." Dr. Hobson then took the Chair, and, thanking the members present for having elected him, asked Lord Kelvin to communicate his promised address "On the Transmission of Force through a Solid."

The vote of thanks to Lord Kelvin for his interesting communication was moved by Dr. Glaisher, and seconded by Dr. Larmor, and carried unanimously. In response to the request of the meeting, voiced by the above named gentlemen, Lord Kelvin promised to write out his remarks for publication in the *Proceedings.*

Dr. Glaisher communicated two papers, viz., (i.) "A General Congruence Theorem relating to the Bernoullian Functions," and (ii.) "On the Residues of Bernoullian Functions for a Prime Modulus, including as special cases the Residues of the Eulerian Numbers and the *I*-Numbers." Major MacMahon asked a question in connection with Sylvester's work in this direction.

Mr. Tucker communicated "Further Notes on Isoscelians," and spoke on the properties of two in-triangles which are similar to the pedal triangle.

The President read the titles of the following papers:—

In a Simple Group of an Odd Composite Order every System of Conjugate Operators or Sub-Groups includes more than Fifty: Dr. G. A. Miller.
Prime Functions on a Riemann Surface: Prof. A. C. Dixon.
On Green's Function for a Circular Disc: H. S. Carslaw.
On the Real Points of Inflexion of a Curve: A. B. Basset.
On Quantitative Substitutional Analysis: Alfred Young.
On a Class of Plane Curves: J. H. Grace.
(i.) On Group Characteristics, and (ii.) On some Properties of Groups of Odd Order: Prof. W. Burnside.
(i.) Conformal Space Transformations, and (ii.) Dynamical and other Applications of Algebra of Bilinear Functions: T. J. I'A. Bromwich.

The following presents were made to the Library:—

"Educational Times," November, 1900.

"Indian Engineering," Vol. xxviii., Nos. 12–15, Sept. 22–Oct. 13, 1900.

"Procès Verbal de la Société des Naturalistes," Années 8, 9, 10; Varsovie, 1898–1899.

Edalji, J.—"Reciprocally related Figures and the Principle of Continuity," 8vo; Ahmedabad, 1900.

"Mathematisch-naturwissenschaftliche Mitteilungen in Württemberg," Serie 2, Bd. ii., Heft 3; Stuttgart, 1900.

"Mathematical Gazette," Vol. i., No. 23; 1900.

Lebon, E.—"Solution de la Problême de Malfatti," 8vo; Coimbra, 1889 (from the "Rendiconti del Circ. Mat. di Palermo").

The following exchanges were received:-

"Proceedings of the American Philosophical Society," Vol. xxxix., No. 162; Philadelphia, 1900.

"Periodico di Matematica," Serie 2, Vol. iii., Fasc. 2; Livorno, 1900.

"Transactions of the American Mathematical Society," Vol. i, No. 3; July, 1900.

"Annals of Mathematics," Series 2, Vol. ii., No. 1; Harvard University, 1900.

"Proceedings of the Royal Society," Vol. lxvii., Nos. 436, 437; 1900.

"Beiblätter zu den Annalen der Physik und Chemie," Bd. xxiv., St. 9; Leipzig, 1900.

"Rendiconti del Circolo Matematico di Palermo," Tomo xiv., Fasc. 5; Sett.-Ott., 1900.

"Bulletin of the American Mathematical Society," Series 2, Vol. vii., No. 1, Oct., 1900; New York.

"Jornal de Sciencias Mathematicas e Astronomicas," Vol. xiv., No. 2; Coimbra, 1900.

"Monatshefte für Mathematik und Physik," Jahrgang xi., Pt. 4; Wien, 1900.

"Bulletin des Sciences Mathématiques," Tome xxiv., Juillet, Août, 1900; Paris.

"Journal für die reine und angewandte Mathematik," Bd. cxxii., Heft 4; Berlin, 1900.

"Archives Néerlandaises," Série 2, Tome iv., Livr. 1; La Haye, 1900.

"Atti della Reale Accademia dei Lincei—Rendiconti," Sem. 2, Vol. ix., Fasc. 7; Roma, 1900.

"Nyt Tidsskrift for Matematik," B. Aargang ii., Nr. 3; Copenhagen, 1900.

"Journal of the Institute of Actuaries," Vol. xxxv., Pt. 5, Oct., 1900.

"Memoirs and Proceedings of the Manchester Literary and Philosophical Society," Vol. xliv., Pt. 5, 1900.

"Nachrichten von der Königl. Gesellschaft der Wissenschaften zu Göttingen," Math.-Phys. Klasse, Heft 2; 1900.

"Tōkyō Sūgaku-Butsurigaku Kwai Kiji," Maki No. 8, Dai 4, 5, 1900.

In a Simple Group of an Odd Composite Order every System of Conjugate Operators or Sub-groups includes more than Fifty.

By G. A. Miller.

Received July 4th, 1900. Read November 8th, 1900.

Burnside has called attention to the importance of the study of questions relating to simple groups of an odd composite order, and he has proved some theorems which throw light on this question.* In what follows this subject is studied from a somewhat different standpoint, and the proof of the theorem stated in the heading is the principal objective point. This theorem is evidently equivalent to the theorem: The degree of a simple group of an odd order must exceed fifty. This proof is based, to a large extent, upon the following facts.

If we represent a simple group of an odd composite order as a substitution group in the smallest possible number (n) of elements, the group (G) is primitive and simply transitive. All its transitive sub-groups, as well as all the transitive constituents of its intransitive sub-groups, are only simply transitive, and of an odd order. In particular, its maximal sub-group of degree $n-1$ (G_1) is composed of an even number of simply transitive constituents of an odd order. The order of each one of these transitive constituents involves all the prime factors that are contained in the order of G_1.†

The degree of G cannot be a prime number of the form 2^a+1, since the operators of this prime order would be transformed into themselves by substitutions of order 2, according to the theorem that each operator of a prime order (p) in a group of degree p must be transformed into itself by more than p operators of the group, whenever the order of the group is composite. If one of the transitive constituents of G_1 were of a prime degree of the form 2^a+1, the order of G_1 would have to be p.‡ In this case G would have to contain just $n-1$ substitutions of degree n, and hence it could be represented as a transitive group whose degree would not exceed $n-1$, a result which is contrary to the hypothesis that G is represented by the smallest possible number of elements. We may therefore assume that G_1 does not contain any transitive constituent whose degree is one of the numbers 3, 5, 17, ...

---

* Burnside, *Theory of Groups of a Finite Order*, 1897, pp. 371, 379.

† Jordan, *Traité des Substitutions*, 1870, p. 284.

‡ *Proc. Lond. Math. Soc.*, Vol. xxviii., p. 536.

By means of the following general theorem we may further restrict the possible degrees of transitive constituents of G_1.

THEOREM.—*If G_1 contains a transitive constituent (of degree n_1) whose order is not divisible by $p^{\alpha+1}$ (p being a prime number), and if this constituent contains a self-conjugate sub-group of order p^α which includes $p^\alpha-1$ substitutions of degree n_1, then the order of G_1 will not be divisible by $p^{\alpha+1}$, whenever the sub-group which corresponds to identity of this constituent is generated by its substitutions of order p^γ, or contains only one maximal group whose order is of the form p^δ.*

We shall prove this theorem by showing that the hypothesis that the order of G_1 is divisible by $p^{\alpha+1}$ leads to a contradiction. Suppose that the order of G_1 is divisible by p^β ($\beta>\alpha$), but not by any higher power of p. All the operators of G_1 whose orders are powers of p generate a sub-group (G_β) of G_1, which has the given self-conjugate sub-group (P_α) of order p^α as a constituent. To identity of P_α there corresponds a self-conjugate sub-group (H) of G_1 whose order is $mp^{\beta-\alpha}$. Some of the conjugates of G_1 contain H without containing any other operator of G_β. When $m=1$ these conjugates of G_1 will clearly contain operators that transform H into itself, but are not contained in G_1.* This is impossible, since G_1 is a maximal sub-group of G. We may therefore assume $m>1$.

All the operators of H whose orders are divisors of m generate a self-conjugate sub-group (M) of G_1 whose order cannot exceed $mp^{\beta-\alpha}$. If the order of M is not divisible by $p^{\beta-\alpha}$, M must be generated by operators whose orders are powers of p, and hence it has to be self-conjugate in the given conjugates of G_1. As this is clearly impossible, it remains only to consider the case when $m>1$, and when the order of m is divisible by $p^{\beta-\alpha}$. In this case the operators of M whose orders are divisible by p generate a self-conjugate sub-group of G_1. As this would also be self-conjugate in the given conjugates of G_1, the theorem is proved. It may be observed that the theorem applies to any simply transitive primitive group of degree n, even if its order is even, G_1 being the maximal sub-group of degree $n-1$.

In what follows we shall assume $n<51$.

---

* Burnside, *Proc. Lond. Math. Soc.*, Vol. XXVI., p. 209.

It is easy to prove that G_1 cannot have a transitive constituent of degree 7. Such a transitive constituent would have to be of order 21, since the cyclic and semi-metacyclic groups are the only two transitive groups of degree 7 which have an odd order. If each of the other transitive constituents of G_1 were also of degree 7, the order of G_1 would clearly be 21. This is impossible, since it is known that there is no simple group whose order is odd and $\leqq 50.21$. Hence we observe that G_1 has to contain a constituent of degree 21 or of degree 27 if it contains a constituent of degree 7. The constituent of degree 27 could not be imprimitive, since a transitive group of an odd order and of degree 9 cannot include any operator of order 7. It could not be primitive, since its maximal sub-group of degree 26 could not be composed of an even number of transitive constituents of degree 7. It remains to consider the case when G_1 contains a transitive constituent of degree 21 and one or more constituents of degree 7.

The constituent of degree 21 could not be regular, since the order of G_1 must exceed 21. It could not be primitive, since the order of its maximal sub-group of degree 20 could not be a power of 3. It could not have seven systems of imprimitivity, since the self-conjugate sub-group of order 3^a which would correspond to identity in the transitive constituent of degree 7 could not be similar to other sub-groups of G_1. As it evidently could not have three systems of imprimitivity, we have proved that G_1 cannot have any transitive constituent of degree 7 if the degree of G does not exceed 50.

We proceed to prove that G_1 cannot have a transitive constituent of degree 9. Such a constituent would have one of the following orders :—9, 27, 81.[*] Hence the order of G would be $3^a n$, and n could be neither a prime number nor the square of a prime.[†] Since G_1 would have either two or four constituents of degree 9, or one constituent of degree 9 and one of degree 27, n would be either 19 or 37, and hence G_1 cannot contain a constituent of degree 9. If it contained a constituent of degree 11 or 13, its order would be 55 or 39 respectively, and the order of G could not exceed 2835.[‡]

We have now proved that G_1 cannot contain any constituent whose degree is less than 15. If it contained two constituents of degree 15, they would be imprimitive,* and the order of G would be $3^\alpha . 5^\beta . 31$ $(\alpha < 10, \beta < 6)$. The number of sub-groups of order 31 would be 125, since this is the only number within the given limits which is congruent to 1, mod 31. The order of G_1 would therefore be $3 . 5^\gamma$ $(\gamma < 5)$, and its sub-group of order 5^γ would be Abelian. As this is clearly impossible, G_1 cannot contain two constituents of degree 15. If G_1 contained two constituents of degrees 15 and 25 respectively, the constituent of degree 25 would be primitive, since an imprimitive group of degree 25 and of odd order cannot include any operator of order 3. It may be observed that this group of order 75 is the first primitive group of an odd order that is not included in a metacyclic group of a prime degree. The order of this constituent would be 75, and it would contain 50 operators of order 3 and degree 24, and 24 operators of degree 25 and order 5. Since the order of G could not be $75 . 31$, this is impossible.

---

[*] *Quart. Jour. of Math.*, Vol. xxvi., 1893, p. 376.

[†] Burnside, *Theory of Groups*, 1897, p. 348. *Cf.* Jordan, *Liouville*, Vol. iv., 1898, p. 21.

[‡] Burnside, *Theory of Groups*, 1897, p. 371.

It was observed above that G_1 cannot contain any constituent of degree 17. If it contained two constituents of degree 19, the order of G would be $39 . 19 . 3^\alpha$ $(\alpha < 3)$. The number of its sub-groups of order 13 would be 27, since this is the only number within the given limits which is congruent to 1, mod 13. This is impossible, since a sub-group of order 13 could not be transformed into itself by an operator of order 19. If G_1 contained two constituents of degree 21, its order would be $7^\alpha . 3^\beta$ $(\alpha = 1, \beta < 16$, or $1 < \alpha < 6, \beta < 8)$.

The number of sub-groups of order 43 in G would therefore be $7 . 3^7 = 356 . 43 + 1$, and the number of sub-groups of order 7 would be $43 . 3^6$. Hence each of the two constituents of G_1 would contain seven systems of imprimitivity. Their sub-groups which would not permute any of the systems of imprimitivity would be composed of cycles of degree 3 in distinct sets of elements, and hence they would be Abelian.

The substitutions of G_1 whose degree is less than 40 would generate a self-conjugate sub-group of order 3^α, all of whose transitive constituents would be of degree 3. This would contain a sub-group of order $3^{\alpha-1}$ which would occur in a conjugate of G_1, and hence it would be transformed into itself by a group of degree 43. As this is impossible, G_1 cannot contain two constituents of degree 21.

It remains to prove that G_1 cannot involve two constituents of degree 23. In this case the order of G_1 would be $23 . 11$, while the order of G would be 23.11.47. This is impossible, since 23.11 is not conjugate to 1, mod 47. We have now examined all possible cases and found that there is no simple group of an odd order whose degree is less than 51. This proves the statement of the heading.

---

* *Proc. Lond. Math. Soc.*, Vol. xxviii., 1897, p. 533.

Prime Functions on a Riemann Surface. *By* A. C. Dixon.

Received August 10th, 1900. Read November 8th, 1900.
Received, in revised form, January 19th, 1901.

In a paper read to the London Mathematical Society (*Proceedings*, Vol. XXXI., p. 308) I pointed out a method by which prime functions quite analogous to the elliptic theta-functions could be introduced into the more general theory of Abelian functions. In the present paper I have gone more fully into the general theory of these prime functions, investigating their relations to each other and giving other methods by which they may be introduced. The discussion is, of course, largely parallel to that in Prof. Klein's paper (*Math. Ann.*, Vol. XXXVI., p. 1) and the corresponding parts of Mr. Baker's book.

1. Take a Riemann surface, resolved by a canonical system of $2p$ cuts into a simply connected surface or polygon, whose boundary in the positive sense when it is opened out is

$$a_1 b_1 c_1 d_1 a_2 b_2 c_2 d_2 \dots a_p b_p c_p d_p;$$

thus $a_i b_i$ and $d_i c_i$ will be opposite sides of the same cut, and so will $c_i b_i$ and $d_i a_{i+1}$ (a_{p+1} being the same as a_1). Let S_i, T_i denote the operations of moving across the polygon from a point of $a_i b_i$ to the corresponding point of $c_i d_i$, and from a point of $b_i c_i$ to the corresponding point of $d_i a_{i+1}$ respectively, or of moving round circuits equivalent to these.

Let $u_1, u_2, \dots, u_p$ be the integrals of the first kind, such that

$$u_i(S_i z) = u_i(z) + 2\iota\pi,$$

$$u_i(S_j z) = u_i(z) \quad (i \neq j),$$

$$u_i(T_j z) = u_i(z) + \omega_{ij},$$

where $$\omega_{ij} = \omega_{ji}.$$

Consider a function $\theta_e(z)$ having no pole or singularity within the polygon or on its boundary, and having one simple zero at e, and affected by passage round the circuits* so that

$$\left.\begin{aligned}\log\theta_e(S_iz) &= \log\theta_e(z)+\sum_j a_{ij}u_j+\beta_i\\ \log\theta_e(T_iz) &= \log\theta_e(z)+\sum_j \gamma_{ij}u_j+\delta_i\end{aligned}\right\}\ (i=1,\,2,\,\ldots,\,p).\quad(1)$$

Such a function will be called a *prime function* in this paper. Functions uniform within the polygon and satisfying relations of the form (1) will be called *factor-functions*, and such as have no pole or zero *accidental factors*. The $2p\,(p+1)$ quantities α, β, γ, δ are not altogether arbitrary, but must satisfy certain relations which can be found as follows. Take for simplicity the case of a prime function.

In the first place $\int d\log\theta_e(z)$ taken round the whole boundary of the polygon must be $2\iota\pi$. But the part of this contributed by the sides a_ib_i and c_id_i is

$$-\int_{a_i}^{b_i} d\log\frac{\theta_e(S_iz)}{\theta_e(z)} = -\sum_j a_{ij}\int_{a_i}^{b_i} du_j = -\sum_j a_{ij}\int_{d_i}^{c_i} du_j = \sum_j a_{ij}\omega_{ij}.$$

The part given by the sides b_ic_i and d_ia_{i+1} is

$$-\int_{b_i}^{c_i} d\log\frac{\theta_e(T_iz)}{\theta_e(z)} = -\sum_j \gamma_{ij}\int_{b_i}^{c_i} du_j = -2\iota\pi\,.\,\gamma_{ii}.$$

Thus, by summation, we have

$$\sum_i \gamma_{ii} = -1+\frac{1}{2\iota\pi}\sum_i\sum_j a_{ij}\omega_{ij}.\qquad(2)$$

Again, the value of $\int u_1 d\log\theta_e(z)$ taken round the whole boundary of the polygon is $2\iota\pi\,.\,u_1(e)$. The part contributed by the sides a_1b_1 and c_1d_1 is

$$\begin{aligned}&\int_{d_1}^{c_1}\left[(u_1-2\iota\pi)\,d\log\theta_e(S_1^{-1}z)-u_1\,.\,d\log\theta_e(z)\right]\\ &\qquad=\int_{d_1}^{c_1}\left[-(u_1-2\iota\pi)\sum_j a_{1j}du_j-2\iota\pi\,d\log\theta_e(z)\right]\\ &\qquad=\sum_j a_{1j}\int_{c_1}^{d_1}u_1\,du_j-2\iota\pi\sum_j a_{1j}\omega_{1j}+2\iota\pi\left\{\sum_j\gamma_{1j}u_j(c_1)+\delta_1\right\}.\end{aligned}$$

---

* Here the circuits S_i, T_i are taken as equivalent to the sides b_ic_i, c_id_i of the polygon respectively, and, if one of the circuits is altered so as to pass on the other side of the point e, the right-hand side of the corresponding equation must be increased or diminished by $2\iota\pi$.

The part given by $a_i b_i$ and $c_i d_i$ $(i \neq 1)$ is

$$\sum_j a \int_{c_i}^{d_i} u_1 \, du \, .$$

The part given by $b_i c_i$ and $d_i a_{i+1}$ $(i = 1, 2, \ldots, p)$ is

$$\int_{b_i}^{c_i} \left[-(u_1 + \omega_{1i}) \, d \log \theta_e \, (T_i z) + u_1 d \log \theta_e \, (z) \right]$$

$$= \int_{b_i}^{c_i} \left[-(u_1 + \omega_{1i}) \sum_j \gamma_{ij} du_j - \omega_{1i} d \log \theta_e \, (z) \right]$$

$$= -\sum_j \gamma_{ij} \int_{b_i}^{c_i} u_1 du_j - \omega_{1i} \gamma_{ii} \, . \, 2\iota\pi - \omega_{1i} \left\{ \sum_j a_{ij} u' \, (b_i) + \beta_i \right\} .$$

Thus we have the relation

$$\delta_1 + \sum_j \gamma_{1j} \, . \, u_j \, (c_1)$$

$$= \frac{1}{2\iota\pi} \sum_i \sum_j \left\{ \gamma_{ij} \int_{b_i}^{c_i} - a_{ij} \int_{c_i}^{d_i} \right\} u_1 du_j + u_1 \, (e) + \frac{1}{2\iota\pi} \sum_i \omega_{1i} \left\{ \beta_i + \sum_j a_{ij} \, u_j (b_i) \right\}$$

$$+ \sum_i \omega_{1i} \, (a_{1i} + \gamma_{ii}) . \qquad (3)$$

This holds also when any of the suffixes 2, ..., p is put in the place of 1, and thus it represents p relations.

The equations (2), (3) hold for factor-functions in general with slight modification. In (2) we must put as the first term on the right the excess in number of the poles over the zeroes of the function. In (3) we must have in place of the term $u_1 \, (e)$ the sum of the values of u_1 at the zeroes diminished by the sum of its values at the poles.

It will be found that there are no more restrictions on the quantities a, β, γ, δ than those expressed in the equations (2), (3) as thus modified, or, say, the equations (2′), (3′).

The ratio of two factor-functions with the same poles and zeroes will be an accidental factor. For any accidental factor the equations (2′), (3′) are linear and homogeneous in the quantities a, β, γ, δ, the coefficients being constants depending on the surface, and also on the fixed place where the cuts begin and end. The dependence on this place is clearly only apparent.

We shall now discuss the question of the existence of factor-functions and their reduction to their simplest forms.

Actual Formation of Accidental Factors and Prime Functions.

2. The simplest accidental factors are those of the forms exp u_i exp u_iu_j. For exp u_i we have

$$\alpha = \gamma = 0 \text{ for all pairs of suffixes},$$

$$\beta_i = 2\iota\pi, \quad \beta_j = 0 \quad (j \neq i),$$

$$\delta_j = \omega_{ij}.$$

Exp u_iu_j is the product of $\exp \int u_i du_j$ and $\exp \int u_j du_i$, each of which is an accidental factor. For we have, as the increase in the logarithm of $\exp \int_{z_0}^{z} u_i du_j$ when z passes round any circuit S,

$$\int_{z_0}^{Sz} u_i du_j - \int_{z_0}^{z} u_i du_j = \int_{Sz_0}^{Sz} u_i du_j + \int_{z_0}^{Sz_0} u_i du_j - \int_{z_0}^{z} u_i du_j$$

$$= \omega \int_{z_0}^{z} du_j + \int_{z_0}^{Sz_0} u_i du_j,\text{*}$$

where ω is the modulus of u_i for the circuit S. Here then $\alpha_{ij} = 2\iota\pi$, $\alpha = 0$ for other pairs of suffixes.

Hence any given factor-function can be expressed as the product of a factor function for which $\alpha = 0$, $\beta = 0$, and functions of the forms $\exp c \int u_i du_j$, $\exp cu_i$, c being constant. For to destroy all the coefficients α we need only divide the given factor-function by

$$\prod_{i,j} \exp \frac{\alpha_{ij}}{2\iota\pi} \int u_i du_j;$$

and, if $\alpha = 0$ for all pairs of suffixes, we destroy β for all suffixes if we divide by

$$\exp \sum_i \beta_i u_i / 2\iota\pi.$$

Now let v_e be such a multiple of V_e, the normal elementary integral of the second kind, with e for pole, that $\int v_e du_i$ taken round a small contour enclosing e has the value $2\iota\pi$. Then the function $\exp \int v_e du_i$ has no pole within the polygon and no zero except a simple one at e, and it is, in fact, a prime function. For take any circuit S, and let η

---

[*] In this and other places where the paths of integration are clearly implied, I have not thought it necessary to take up space by defining them. Any place on the surface is, in fact, throughout supposed to be reached by a definite path from a fixed origin.

denote the modulus of v_e for this circuit. Then when z passes round the circuit $\int_{z_0}^{z} v_e du_i$ is changed into $\int_{z_0}^{Sz} v_e du_i$, the increment of this integral being*

$$\int_{z_0}^{Sz_0} v_e du_i + \left\{ \int_{Sz_0}^{Sz} - \int_{z_0}^{z} \right\} v_e du_i = \int_{z_0}^{Sz_0} v_e du_i + \int_{z_0}^{z} \eta \, du_i$$

$$= \eta \, u_i(z) + \int_{z_0}^{Sz_0} v_e du_i - \eta \, u_i(z_0).$$

Since this holds for any circuit, the function is a prime function, and we have, moreover,

$$a = 0 \text{ for all pairs of suffixes,}$$

$$\gamma_{ji} = \text{modulus of } v_e \text{ for the circuit } T_j,$$

$$\gamma_{jh} = 0 \quad (h \neq i).$$

There is an exception to this if e is one of the $2p-2$ zeroes of du_i. Then $\int V_e du_i$ is finite at e, as elsewhere, and $\exp \int V_e du_i$ is an accidental factor, not a prime function. The rest of the investigation holds good, so that γ_{ji} is proportional to the differential coefficient of u_j at e, and

$$\gamma_{ii} = 0, \quad \gamma_{jh} = 0 \;\; (h \neq i), \;\; a = 0 \text{ for all pairs of suffixes.}$$

In this way $2p-2$ functions can be formed, one for each of the points at which du_i vanishes. Of the $2p-2$ sets of $p-1$ coefficients γ_{ji} $(j \neq i)$ thus got, $p-1$ must be linearly independent, since otherwise a linear combination of $du_1, du_2, \ldots, du_{i-1}, du_{i+1}, \ldots, du_p$ would vanish at the same $2p-2$ points as du_i, and could therefore only be a constant multiple of du_i, which is impossible. Thus, again, by dividing by accidental factors of the form $\exp c \int V_e du_i$, where c is a constant and e is one of the zeroes of du_i, we can destroy the coefficients γ_{ji}, except γ_{ii}, in any given factor-function.

Now let U stand for $u_1 + u_2 + \ldots + u_p$, and let e be one of the zeroes of dU. Then $\exp \int V_e dU$ is another accidental factor for which $a = 0$ in all cases, and $\gamma_{ji} =$ modulus of V_e for the circuit T_j $(i = 1, 2, \ldots, p)$.

---

* This proof is repeated from *Proc. Lond. Math. Soc.*, Vol. XXXI., pp. 308, 309. It should be noted that the passage on p. 309, from "Suppose now" to "arbitrary zero" is faulty. A better investigation is given below (see the end of § 3).

Since e is a zero of dU, the sum of the moduli of V_e for the circuits $T_1, T_2, \ldots, T_p$ must be zero, and thus

$$\gamma_{11}+\gamma_{22}+\ldots+\gamma_{pp}=0.$$

This is, however, the only linear relation satisfied by the moduli of V_e, since, as before, $p-1$ of the $2p-2$ sets of moduli corresponding to the different zeroes of dU must be linearly independent. Hence we have here $p-1$ more special accidental factors by means of which all but one of the quantities

$$\gamma_{11}, \gamma_{22}, \ldots, \gamma_{pp}$$

can be destroyed in any given factor-function.

Thus, given any accidental factor whatever, we can by dividing it by suitable powers of certain known special accidental factors reduce it to an accidental factor in which, first, $\alpha=0$ for all pairs of suffixes, then $\gamma_{22}, \gamma_{33}, \ldots, \gamma_{pp}$ vanish, then $\gamma=0$ for all pairs of unequal suffixes, then $\beta=0$ for all suffixes; so that finally of all the quantities $\alpha, \beta, \gamma, \delta$ only $\gamma_{11}, \delta_1, \delta_2, \ldots, \delta_p$ are left.

But the relation (2′) for an accidental factor shows that now $\gamma_{11}=0$ also, and from (3′) we have $\delta_1=\delta_2=\ldots=\delta_p=0$. Thus the accidental factor is now reduced to a function uniform on the surface and without pole or zero, that is, to a constant. Or the result may be stated thus—it is possible to construct an accidental factor for which all the quantities α, β, and all the quantities γ except γ_{11}, shall be assigned arbitrarily.

Again, we have seen that $\exp\int v_e\, du_i$ is a prime function with the arbitrary zero e; by means of products and quotients of such prime functions it is possible to construct factor-functions with all zeroes and poles assigned. By means of the special accidental factors that have been investigated the quantities $\alpha, \beta, \gamma, \delta$ for any factor-function can be altered in any way consistent with the equations (2′), (3′).

Thus, finally, *it is possible to construct a factor-function with all zeroes and poles assigned, and such that the quantities* $\alpha, \beta, \gamma, \delta$ *shall have any assigned values satisfying the conditions* (2′), (3′), $p+1$ in number.

3. Let the *degree* of a factor-function be the excess of the number of its zeroes over that of its poles. We shall consider such a function to be *reduced* when α, β vanish for all suffixes, $\gamma=0$ for unequal

suffixes, $\gamma_{11} = \gamma_{22} = \dots = \gamma_{pp} = -\frac{1}{p}$ of the degree of the function. Thus reduced factor-functions are formed by multiplication and division from the proper reduced prime functions without any accidental factor.

A reduced factor-function of degree 0 will thus be a factorial function; the factors for the circuits $S_1, S_2, \dots, S_p$ will all be unity. The factor for the circuit T_i will be $\exp \delta_i$, that is,

$$\exp\left\{\Sigma u_i(e) - \Sigma u_i(f)\right\},$$

where e denotes one of the zeroes and f one of the poles. If, then,

$$\Sigma u_i(e) = \Sigma u_i(f) \quad (i = 1, 2, \dots, p),$$

the reduced factor-function of degree 0 will be an algebraic function.

When $$\Sigma u_i(e) - \Sigma u_i(f) = 0 \quad (i = 1, 2, \dots, p)$$

for two sets of places e, f, the same in number, we shall say that the two sets are *strictly* coresidual. They are coresidual in the ordinary sense when these expressions differ from zero by a period. Thus any two coresidual sets may be made strictly so by passing any place of one set round a suitable circuit; the word "strictly" implies a restriction on the paths by which we may pass from the one set of points to the other.

It may be well to note further that, for the reduced prime function $\theta_e(z)$,

$$\delta_i = \frac{1}{p} u_i(c_i) - \frac{1}{2p\iota\pi} \sum_j \int_{b_j}^{c_j} u_i \, du_j - \frac{1}{p} \sum_j \omega_{ij} + u_i(e).$$

4. Let us now take two reduced prime functions, $\theta_e(z)$ and $\theta_f(z)$, having zeroes at e, f respectively. Let $\epsilon_1, \epsilon_2, \dots, \epsilon_p$ be the quantities corresponding to $\delta_1, \delta_2, \dots, \delta_p$ in the case of $\theta_f(z)$. Let us add to the boundary of the polygon a small closed contour enclosing e and a cut joining this contour to the old boundary at a_1. Then $2\iota\pi \log \theta_e(f)$ will be the value of

$$\int \log \theta_e(z) \, d \log \theta_f(z),$$

taken round the boundary as thus increased.

Now, the part contributed by $a_i b_i$ and $c_i d_i$ is zero. From $b_i c_i$ and $d_i a_{i+1}$ we have

$$\int_{b_i}^{c_i} \Big[\log\theta_e(z)\, d\log\theta_f(z) - \Big\{ \log\theta_e(z) - \frac{1}{p} u_i + \delta_i \Big\} \Big\{ d\log\theta_f(z) - \frac{1}{p} du_i \Big\} \Big]$$

$$= \frac{1}{p} \int_{b_i}^{c_i} \{ u_i d\log\theta_f(z) + \log\theta_e(z)\, du_i \} - \frac{1}{p^2} \int_{b_i}^{c_i} (u_i - p\delta_i)\, du_i$$

$$= \frac{1}{p} \int_{b_i}^{c_i} \{ \log\theta_e(z) - \log\theta_f(z) \}\, du_i + \frac{2\iota\pi}{p} \log\theta_f(c_i) - \frac{2\iota\pi}{p^2} \{ u_i(c_i) - p\delta_i - \iota\pi \}.$$

Now $$\log\theta_f(c_i) - \frac{1}{p} u_i(c_i) + \epsilon_i = \log\theta_f(d_i) = \log\theta_f(a_i).$$

It is also equal to

$$\log\theta_f(b_i) - \frac{1}{p} u_i(b_i) + \epsilon_i - \frac{2\iota\pi}{p} = \log\theta_f(a_{i+1}) - \frac{2\iota\pi}{p}.$$

Thus

$$\log\theta_f(a_i) = \log\theta_f(a_{i-1}) + \frac{2\iota\pi}{p} = \ldots = \log\theta_f(a_1) + \frac{2(i-1)\iota\pi}{p},$$

and the part of the integral given by $b_i c_i$ and $d_i a_{i+1}$ is

$$\frac{1}{p} \int_{b_i}^{c_i} \{ \log\theta_e(z) - \log\theta_f(z) \}\, du_i + \frac{2\iota\pi}{p} \Big\{ \log\theta_f(a_1) + \delta_i - \epsilon_i + \frac{(2i-1)\iota\pi}{p} \Big\}.$$

The integral round the contour enclosing e tends to zero when the contour is indefinitely diminished. From the two sides of the cut joining this to a_1, we have in the limit

$$2\iota\pi \int_{a_1}^{e} d\log\theta_f(z),$$

that is, $$2\iota\pi \{ \log\theta_f(e) - \log\theta_f(a_1) \}.^*$$

Hence $$2\iota\pi \log\theta_e(f)$$

$$= 2\iota\pi \{ \log\theta_f(e) - \theta_f(a_1) \} + \frac{1}{p} \sum_i \int_{b_i}^{c_i} \{ \log\theta_e(z) - \log\theta_f(z) \}\, du_i + 2\iota\pi \{ \log\theta_f(a_1) + \iota\pi \} + \frac{2\iota\pi}{p} \sum_i (\delta_i - \epsilon_i).$$

---

* The value of $\log\theta_f(a_1)$ which occurs here may be taken to differ by a multiple of $2\iota\pi$ from that in the last expression. This will have no effect on the final result, since $2\iota\pi$ is the period of the exponential function.

or
$$\log\theta_e(f)-\log\theta_f(e)$$
$$=\iota\pi+\frac{1}{2\iota\pi p}\sum_i\int_{b_i}^{c_i}\{\log\theta_e(z)-\log\theta_f(z)\}\,du_i+\frac{1}{p}\sum_i(\delta_i-\epsilon_i).$$

Now, in $\theta_e(z)$ we still have at disposal a factor independent of z, and this may be so chosen that
$$\frac{1}{2\iota\pi p}\sum_i\int_{b_i}^{c_i}\log\theta_e(z)\,du_i+\frac{1}{p}\sum_i\delta_i$$
shall be independent of e.* It will therefore be equal to
$$\frac{1}{2\iota\pi p}\sum_i\int_{b_i}^{c_i}\log\theta_f(z)\,du_i+\frac{1}{p}\sum_i\epsilon_i,$$
and the right-hand side of the equation last written will reduce to its first term.

We have then after this special determination, say of the value of $\theta_e(z)$ at some fixed place,
$$\log\theta_e(f)=\log\theta_f(e)+\iota\pi$$
and
$$\theta_e(f)=-\theta_f(e).$$

A reduced prime function with this property will be called *normal*. It still contains an arbitrary constant factor independent of the parametric place. We shall have no occasion at present to assign this factor.

The effect on $\log\theta_e(f)$ of a passage of the parametric place round a closed circuit can now be ascertained. If we suppose $\theta_e(z)$ still to denote the normal prime function, we have
$$\log\theta_{S_ie}(f)=\log\theta_e(f),$$
$$\log\theta_{T_ie}(f)=\log\theta_e(f)-\frac{1}{p}u_i(e)+\epsilon_i$$
$$=\log\theta_e(f)-\frac{1}{p}u_i(e)+u_i(f)$$
+a quantity independent of e, f, by (3).

---

* This would, of course, not be true if $\sum_i\int_{b_i}^{c_i}\log\theta_e(z)\,du_i$ were unaffected by the change of $\theta_e(z)$ into $\lambda\theta_e(z)$, λ being a factor independent of z. But this expression would, in fact, be increased through the change by $\log\lambda\sum_i\int_{b_i}^{c_i}du_i$, that is, $2p\iota\pi\log\lambda$.

Hence $\theta_{T_i e}(z)$ may be considered as a prime function with e as parameter; but it is then not reduced, since its logarithm is changed by $2\iota\pi$ when z describes the circuit S_i. Or we may put the matter in another way, and say that a prime function is reduced if β, instead of vanishing, is a multiple of $2\iota\pi$ for all suffixes, the other criteria being unchanged. The parametric place will then be outside the polygon, and will be derived from the zero within the polygon by passage round a circuit made up of T_1 travelled $\beta_1/2\iota\pi$ times, T_2 travelled $\beta_2/2\iota\pi$ times, and so on, and $S_1, S_2, \ldots, S_p$ any number of times.

5. Let
$$(e, e_1, e_2, \ldots, e_p),$$
$$(f, f_1, f_2, \ldots, f_p),$$
$$(g, g_1, g_2, \ldots, g_p)$$
be three strictly coresidual sets of $p+1$ places belonging to a singly infinite series of sets in which no place is common to all. Let θ henceforth denote the normal prime function.

Then the ratios
$$\theta_e(z)\,\Pi\theta_{e_i}(z) : \theta_f(z)\,\Pi\theta_{f_i}(z) : \theta_g(z)\,\Pi\theta_{g_i}(z)$$
are algebraic functions of the place z, by § 3. Thus
$$\{\mu\theta_f(z)\,\Pi\theta_{f_i}(z)+\nu\theta_g(z)\,\Pi\theta_{g_i}(z)\}\div\theta_e(z)\,\Pi\theta_{e_i}(z)$$
is an algebraic function of the place z: by proper choice of the ratio $\mu:\nu$ its numerator may be made to vanish when $z=e$, so that the expression must be constant, as it cannot have poles at $e_1, \ldots, e_p$ only. Hence there is an equation of three terms
$$\lambda\theta_e(z)\,\Pi\theta_{e_i}(z)+\mu\theta_f(z)\,\Pi\theta_{f_i}(z)+\nu\theta_g(z)\,\Pi\theta_{g_i}(z)=0,$$
where λ, μ, ν are independent of z. For convenience, write this
$$A\theta_f(g)\,\theta_e(z)\,\Pi\theta_{e_i}(z)+B\theta_g(e)\,\theta_f(z)\,\Pi\theta_{f_i}(z)+C\theta_e(f)\,\theta_g(z)\,\Pi\theta_{g_i}(z)=0.$$

Then, by putting e, f, g for z in succession, we have
$$B : C :: \prod_i \theta_e(g_i) : \prod_i \theta_e(f_i),$$
$$C : A :: \prod_i \theta_f(e_i) : \prod_i \theta_f(g_i),$$
$$A : B :: \prod_i \theta_g(f_i) : \prod_i \theta_g(e_i).$$

Thus $\prod_i \theta_e(g_i) \prod_i \theta_f(e_i) \prod_i \theta_g(f_i) = \prod_i \theta_e(f_i) \prod_i \theta_f(g_i) \prod_i \theta_g(e_i).$

To put A, B, C in a symmetrical form, we may introduce a fourth series of coresidual places

$$(h, h_1, \ldots, h_p).$$

Then we have from the relation last written

$$\Pi\theta_e(g_i)\,\Pi\theta_f(e_i)\,\Pi\theta_h(f_i)\,\Pi\theta_g(h_i) = \Pi\theta_e(f_i)\,\Pi\theta_f(h_i)\,\Pi\theta_h(g_i)\,\Pi\theta_g(e_i),$$

and thus

$$\begin{aligned} B : C &:: \Pi\theta_e(g_i) : \Pi\theta_e(f_i) \\ &:: \Pi\theta_f(h_i)\,\Pi\theta_h(g_i)\,\Pi\theta_g(e_i) : \Pi\theta_f(e_i)\,\Pi\theta_h(f_i)\,\Pi\theta_g(h_i) \\ &:: \left\{\Pi\theta_e(g_i)\,\Pi\theta_g(e_i)\frac{\Pi\theta_f(h_i)}{\Pi\theta_h(f_i)}\right\}^{\frac{1}{2}} : \left\{\Pi\theta_f(e_i)\,\Pi\theta_e(f_i)\frac{\Pi\theta_g(h_i)}{\Pi\theta_h(g_i)}\right\}^{\frac{1}{2}}. \end{aligned}$$

It is clear that these square roots are only surds in appearance; if, for instance, e coincides with g_1, so that $\Pi\theta_e(g_i)$ vanishes, then g will coincide with one of the series $e_1, \ldots, e_p$, so that the product $\Pi\theta_e(g_i)\,\Pi\theta_g(e_i)$ will vanish doubly.

Thus the equation of three terms takes the symmetrical form

$$\begin{aligned} &\left\{\Pi\theta_f(g_i)\,\Pi\theta_g(f_i)\frac{\Pi\theta_e(h_i)}{\Pi\theta_h(e_i)}\right\}\theta_f(g)\,\theta_z(e)\,\Pi\theta_z(e_i) \\ &+\left\{\Pi\theta_g(e_i)\,\Pi\theta_e(g_i)\frac{\Pi\theta_f(h_i)}{\Pi\theta_h(f_i)}\right\}^{\frac{1}{2}}\theta_g(e)\,\theta_z(f)\,\Pi\theta_z(f_i) \\ &+\left\{\Pi\theta_e(f_i)\,\Pi\theta_f(e_i)\frac{\Pi\theta_g(h_i)}{\Pi\theta_h(g_i)}\right\}^{\frac{1}{2}}\theta_e(f)\,\theta_z(g)\,\Pi\theta_z(g_i) = 0. \end{aligned}$$

If, now, we take z to coincide with h, the relation becomes completely skew symmetrical in e, f, g, h, as follows:—

$$\begin{aligned} &\{\Pi\theta_f(g_i)\,\Pi\theta_g(f_i)\,\Pi\theta_e(h_i)\,\Pi\theta_h(e_i)\}^{\frac{1}{2}}\theta_f(g)\,\theta_e(h) \\ &+\{\Pi\theta_g(e_i)\,\Pi\theta_e(g_i)\,\Pi\theta_f(h_i)\,\Pi\theta_h(f_i)\}^{\frac{1}{2}}\theta_g(e)\,\theta_f(h) \\ &+\{\Pi\theta_e(f_i)\,\Pi\theta_f(e_i)\,\Pi\theta_g(h_i)\,\Pi\theta_h(g_i)\}^{\frac{1}{2}}\theta_e(f)\,\theta_g(h) = 0. \end{aligned}$$

In the same way, if we have a q-ply infinite series of strictly coresidual sets of r places, and if $q+2$ sets

$$a_{1i}, a_{2i}, \ldots, a_{ri} \quad (i = 1, 2, \ldots, q+2)$$

of the system are taken, there will be a homogeneous linear relation among the $q+2$ functions

$$\prod_{j=1}^{r} \theta_z(a_{ji}),$$

the coefficients in this relation being independent of z.

6. The following particular case of this theorem leads to an interesting result.

Take a p-ply infinite series of strictly coresidual sets of $2p$ places, and suppose one of the sets to include the $2p-2$ zeroes of an integrand of the first kind, and two other places ξ, η. Then, in all, p independent sets will be of the same nature, and we may, in fact, take them as

$$\xi,\ \eta,\ e_{i1},\ e_{i2},\ \ldots,\ e_{i,\,2p-2}\quad (i=1,\,2,\,\ldots,\,p)$$

where e_{i1}, e_{i2}, ... are the zeroes of du_i.

Let two other sets of the series be

$$x_1,\ x_2,\ \ldots,\ x_{2p}\,;$$

$$y_1,\ y_2,\ \ldots,\ y_{2p}.$$

Then there must be an identity of the form

$$A\prod_{h=1}^{2p}\theta_z(x_h)+B\prod_{h=1}^{2p}\theta_z(y_h)+\sum_{i=1}^{p}C_i\theta_z(\xi)\,\theta_z(\eta)\prod_{j=1}^{2p-2}\theta_z(e_{ij})=0.$$

From this, by putting $z=\xi$, η, in turn, we get

$$A\prod_{h=1}^{2p}\theta_\xi(x_h)+B\prod_{h=1}^{2p}\theta_\xi(y_h)=0,$$

$$A\prod_{h=1}^{2p}\theta_\eta(x_h)+B\prod_{h=1}^{2p}\theta_\eta(y_h)=0.$$

Now, A, B cannot both vanish, since that would lead to a linear relation among du_1, du_2, ..., du_p.

Hence we have

$$\prod_{h=1}^{2p}\theta_\xi(x_h)/\theta_\eta(x_h)=\prod_{h=1}^{2p}\theta_\xi(y_h)/\theta_\eta(y_h)=Q(\xi,\,\eta),\text{ say.}$$

Thus, so long as ξ, η stay within the polygon, $Q(\xi,\eta)$ is a uniform function of them; for x_1, ..., x_{2p} and y_1, ..., y_{2p} are any two sets of $2p$ places strictly coresidual with ξ, η, e_{11}, e_{12}, ..., $e_{1,\,2p-2}$, and if ξ, for instance, travels to a new position without leaving the polygon, the new value of $Q(\xi,\eta)$ will only depend on the new position of ξ, and not on the path by which it has been reached. Also none of the places x_1, ..., x_{2p} need ever be supposed to coincide with ξ or η, and thus $Q(\xi,\eta)$ is never zero or infinite. Its logarithm is then a uniform function of ξ, η within the polygon.

Suppose, now, that ξ passes round the circuit S_i. Then the new set of places corresponding to x_1, x_2, ..., x_{2p} will be strictly coresidual with

$$S_i\,x_1,\ x_2,\ \ldots,\ x_{2p},$$

and thus it readily follows that

$$Q(S_i\xi, \eta) = Q(\xi, \eta),$$

$$\log Q(S_i\xi, \eta) - \log Q(\xi, \eta) = \text{a multiple of } 2\iota\pi.$$

The change in the logarithm of $Q(\xi, \eta)$ is not necessarily zero, because the paths leading from the set of places

$$x_1, x_2, \ldots, x_{2p}$$

to $$S_i x_1, x_2, \ldots, x_{2p},$$

in whatever order these latter are to be taken, may enclose η or intersect the path of ξ.

Let $$\log Q(S_i\xi, \eta) - \log Q(\xi, \eta) = 2k_i\iota\pi.$$

Then k_i is a definite integer, since $\log Q(\xi, \eta)$ is not affected when ξ describes any circuit on the surface that can be reduced to a point by continuous variation.

Now, suppose ξ to pass round the circuit T_i. The new set taking the place of $x_1, x_2, \ldots, x_{2p}$ will then be strictly coresidual with

$$T_i x_1, x_2, \ldots, x_{2p}.$$

Hence $$\frac{Q(T_i\xi, \eta)}{Q(\xi, \eta)} = \frac{\theta_{T_i\xi}(T_i x_1)}{\theta_{T_i\xi}(x_1)} \frac{\theta_\eta(x_1)}{\theta_\eta(T_i x_1)} \prod_{h=1}^{2p} \frac{\theta_{T_i\xi}(x_h)}{\theta_\xi(x_h)}$$

$$= \exp\left[u_i(T_i\xi) - u_i(\eta) + 2p\left(-\frac{1}{p}\right) u_i(\xi) + \sum_{h=1}^{2p} u_i(x_h) + 2u_i(c_i) \right.$$
$$\left. - \frac{1}{\iota\pi} \sum_{j=1}^{p} \int_{b_j}^{c_j} u_i\,du_j - 2\sum_{j=1}^{p} \omega_{ij}\right]$$

$$= \exp\left[\sum_{h=1}^{2p} u_i(x_h) - u_i(\xi) - u_i(\eta) + 2u_i(c_i) - \frac{1}{\iota\pi} \sum_{j=1}^{p} \int_{b_j}^{c_j} u_i\,du_j - 2\sum_{i=1}^{p} \omega_{ij} + \omega_{ii}\right],$$

a constant quantity.

Thus $\log Q(\xi, \eta)$ is a function of ξ, uniform, finite, and continuous within the polygon, and increased by a constant when ξ passes round any of the circuits $S_1, \ldots, S_p, T_1, \ldots, T_p$. The moduli of periodicity for the circuits $S_1, \ldots, S_p$ are, in fact, zero for the function

$$\log Q(\xi, \eta) - \sum_{i=1}^{p} k_i u_i(\xi).$$

This is therefore independent of ξ. To find its value put $\xi = \eta$. Since $Q(\eta, \eta)$ is clearly 1, we find that in general

$$Q(\xi, \eta) = \exp \sum_{i=1}^{p} k_i \{u_i(\xi) - u_i(\eta)\}.$$

Here $k_1, k_2, \ldots, k_p$ are integers, and they may be reduced to zero by passing one or more of the points $x_1, \ldots, x_{2p}$ round suitable circuits; for instance, x_1 may be passed round T_1 $-k_1$ times, T_2 $-k_2$ times, $\ldots$, T_p $-k_p$ times, and $S_1, S_2, \ldots, S_p$ any number of times.

Thus we have the equation

$$\prod_{h=1}^{2p} \theta_\xi (x_h) = \prod_{h=1}^{2p} \theta_\eta (x_h);$$

this holds when the p expressions

$$\sum_{h=1}^{2p} u_i (x_h) - u_i (\xi) - u_i (\eta)$$

have values differing from certain definite quantities by multiples of $2\iota\pi$ only. These quantities are found from the consideration of $Q(T_i\xi, \eta)$. We must, in fact, have

$$\sum_{h=1}^{3p} u_i(x_h) - u_i(\xi) - u_i(\eta) \equiv \frac{1}{\iota\pi} \sum_{j=1}^{p} \int_{b_j}^{c_j} u_i du_j - 2u_i(c_i) + 2\sum_{j=1}^{p} \omega_{ij} - \omega_{ii} \pmod{2\iota\pi}$$
$$(i = 1, 2, \ldots, p).$$

7. An important expression is that which vanishes when p given places are zeroes of the same integrand of the first kind.

Let e_{ij} $(j = 1, 2, \ldots, 2p-2)$ again denote a zero of du_i, the sets of zeroes for different values of i being strictly coresidual. Let $\varpi_i(z)$ stand for $\prod_{j=1}^{2p-2} \theta_z(e_{ij})$. Then $\varpi_i(z)/\varpi_j(z)$ can only differ by a constant factor from du_i/du_j.

Hence the determinant of order p in which the i-th constituent of the j-th row is $\varpi_i(z_j)$ vanishes if two of the places $z_1, \ldots, z_p$ coincide, or if they are all zeroes of the same integrand of the first kind. The result of dividing this determinant by $\prod_{i=2}^{p} \prod_{j=1}^{i-1} \theta_{z_i}(z_j)$ will be such an expression as is sought; it will be a reduced factor-function of degree $p-1$ of each of the places $z_1, z_2, \ldots, z_p$, without poles.

Let this function be denoted by $\Phi(z_1, z_3, \ldots, z_p)$. Then, if

$$z_{1i} \; (i = 1, 2, \ldots, p-1)$$

is one of the other zeroes of that integrand of the first kind which vanishes at $z_2, z_3, \ldots, z_p$, so that

$$z_2, z_3, \ldots, z_p, z_{11}, z_{12}, \ldots, z_{1,p-1}$$

are strictly coresidual with the zeroes taken for du_i above, the product $\prod_{i=1}^{p-1} \theta_{z_1}(z_{1i})$ will differ from $\Phi(z_1, z_2, \ldots, z_p)$ by a factor independent of z_1, and so by symmetry for $z_2, \ldots, z_p$.

The product $\Phi(z_1, z_2, \ldots, z_p) \prod_{i=1}^{p} \theta_z(z_i)$ can only differ by a factor independent of $z, z_1, \ldots, z_p$ from Riemann's theta-function of the arguments

$$u(z) - \sum_i u(z_i) - u(k) + \sum_i u(k_i),$$

where $k, k_1, \ldots, k_p$ are suitably chosen places, such that $(e_{i1}, \ldots, e_{i2p-2}, k^2)$ are coresidual to $(k_1^2, k_2^2, \ldots, k_p^2)$.

For the two functions vanish together, and are altered by the same factor when any one of the places $z, z_1, \ldots, z_p$ describes a closed circuit. (Compare Klein, *Math. Ann.*, XXXVI., p. 39.)

8. It is clear that the normal elementary integral of the third kind is

$$-\log \frac{\theta_a(x)\,\theta_b(y)}{\theta_a(y)\,\theta_b(x)}$$

if a, b are the parametric places, x, y the limits.

There is thus no need to dwell on the construction of factorial functions as products of prime functions and their powers. The formula given on p. 396 of Mr. Baker's *Abelian Functions* leads directly to the construction in question. The following modified form of the result given in the same work at p. 426 may be of interest:—

Let there be a $(q-1)$-ply infinite series of strictly coresidual sets of r places, so that $r - q + 1 \not> p$ and $= p - s$, say.

Take q independent sets from the series, say

$$e_{i1}, e_{i2}, \ldots, e_{ir} \quad (i = 1, 2, \ldots, q).$$

Then the ratios of the q expressions

$$\prod_{j=1}^{r} \theta_z(e_{ij}) \quad (i = 1, \ldots, q)$$

are algebraic functions of z, and some linear function of them will vanish in all the r places of any set belonging to the system.

Hence, if there are any q places $z_1, z_2, \ldots, z_q$, and we denote by $\Psi(z_1, z_2, \ldots, z_q)$, the quotient of the determinant of the q-th order in which the i-th constituent of the h-th row is

$$\prod_{j=1}^{r} \theta_{z_h}(e_{ij})$$

by the product $$\prod_{i=j}^{q-1} \prod_{j=i+1}^{q} \theta_{z_i}(z_j),$$

then the vanishing of $\Psi(z_1, z_2, \ldots, z_q)$ is the necessary and sufficient condition that $z_1, z_2, \ldots, z_q$ should belong to a set of the system. Also $\Psi(z_1, \ldots, z_q)$ is a factor-function of each of the q places z. As a function, say of z_1, it has no poles and $r-q+1$, that is, $p-s$, zeroes, namely, the other places $z_{11}, z_{12}, \ldots, z_{1,p-s}$ belonging to that set of the system which contains $z_2, z_3, \ldots, z_q$.

Thus $\Psi(z_1, z_2, \ldots, z_q) \prod_{i=1}^{s} \theta_{f_i}(z_1)$, if $f_1, f_2, \ldots, f_s$ are any places, is a function of z_1, having p zeroes, the same as those of

$$\Theta\left\{u(z_1) - u(z_{11}) - u(z_{12}) \ldots - u(z_{1,p-s}) - u(f_1) \ldots - u(f_s) \right.$$
$$\left. - u(k) + u(k_1) + \ldots + u(k_p)\right\},$$

that is, of $\Theta\left\{u(z_1) + u(z_2) + \ldots + u(z_q) - u(f_1) \ldots - u(f_s) - U\right\}$,

where U denotes the quantity

$$\sum_{j=1}^{r} u(e_{ij}) + u(k) - \sum_{j=1}^{p} u(k_j),$$

which by hypothesis is the same for all suffixes i.

Also, the behaviour of these two functions when z_1 passes round any closed circuit is the same, since each is a reduced factor-function.* Thus the two can only differ by a factor independent of z_1, and, by symmetry, $\Psi(z_1, \ldots, z_q) \prod_{i=1}^{s} \prod_{j=1}^{q} \theta_{f_i}(z_j)$ can only differ from

$$\Theta\left\{u(z_1) + u(z_2) + \ldots + u(z_q) - u(f_1) - \ldots - u(f_s) - U\right\}$$

by a factor independent of $z_1, z_2, \ldots, z_q$.

9. There are other ways of introducing the prime function than the one used in this paper. For instance, the prime form of Schottky and Klein (Baker, *Abelian Functions*, chapters xii., xiv.) would, on division by a *Mittelform* (Klein, *Math. Ann.*, XXXVI., pp. 14–17) of the same dimensions, yield a prime function.

Again, take the special transcendent $T_{\xi\eta}(x_1, x_2, \ldots, x_p)$ of Clebsch and Gordan (see also Nöther, *Math. Ann.*, XXXVII., p. 491), that is, the expression

$$\tfrac{1}{2} \sum_{i=1}^{p} \Pi_{\xi, \eta}^{x_i, x'},$$

---

* It may be necessary to pass one of the points $k_1, \ldots, k_p$ round a closed circuit to ensure that the change in the logarithm shall be always the same for both functions.

where $x_1, x_2, \ldots, x_p, x_1', x_2', \ldots, x_p'$ are coresidual with ξ, η, and the zeroes of du_i ($\xi\eta$ *zugeordnet*), and Π denotes an integral of the third kind; we shall suppose it to be the normal integral. Then, since

$$\Pi_{\xi, \eta}^{x, x'} = -\log \frac{\theta_\xi(x)\, \theta_\eta(x')}{\theta_\xi(x')\, \theta_\eta(x)},$$

and $\theta_\xi(x_1)\, \theta_\xi(x_2) \ldots \theta_\xi(x_p)\, \theta_\xi(x_1')\, \theta_\xi(x_2') \ldots \theta_\xi(x_p')$

$$= \theta_\eta(x_1) \ldots \theta_\eta(x_p)\, \theta_\eta(x_1') \ldots \theta_\eta(x_p'),$$

as we have seen above (§ 6), we have

$$T_{\xi\eta}(x_1, x_2, \ldots, x_p) = -\log \prod_{i=1}^{p} \frac{\theta_\xi(x_i)}{\theta_\eta(x_i)}.$$

Suppose now that $x_1, x_2, \ldots, x_p$ are all coincident and fixed, and that η is also fixed; then the prime function $\theta_e(\xi)$ differs by a constant factor from

$$\exp\left\{ -\frac{1}{p} T_{\xi\eta}(e^p) \right\}.$$

Again, a property of Riemann's theta-function, given at p. 255 of Baker's *Abelian Functions*, is, in the notation there used, that the zeroes of

$$\Theta\left(v^{x, m} - v^{z_1, m_1} - v^{z_2, m_2} \ldots - v^{z_p, m_p}\right),$$

regarded as a function of x, are the the places $z_1, z_2, \ldots, z_p$. If we suppose $z_1, z_2, \ldots, z_p$ to coincide, then this function Θ has no poles, and it has only one p-ple zero; so that its p-th root is uniform within the polygon. Also, in regard to the closed circuits on the surface, the p-th root behaves like a prime function [Baker, p. 249 (B)]. So, in fact, it is a prime function of x. In this case, as in that of the function formed by means of the special transcendent $T_{\xi\eta}(x)$, a factor independent of the argument place must be introduced if the function is to have the property

$$\theta_e(f) = -\theta_f(e).$$

A General Congruence Theorem relating to the Bernoullian Function. *By* J. W. L. Glaisher. Read and received November 8th, 1900.

1. In a paper* communicated to the Society on May 10th the values of the residues of the Bernoullian functions $r^{2n+1}B_{2n+1}\left(\frac{l}{r}\right)$ and $r^{2n+1}A'_{2n+1}\left(\frac{l}{r}\right)$, mod p, were obtained in the case when $p-1$ is a divisor of $2n$, the principal formulæ being

$$r^p B_p\left(\frac{l}{r}\right) \equiv l - \left[\frac{l}{p}\right]_r, \text{ mod } p,$$

$$r^p A'_p\left(\frac{l}{r}\right) \equiv \left[\frac{l}{p}\right]_{2r} - \left[\frac{l}{p}\right]_r, \text{ mod } p,$$

where p is any uneven prime number, r is any number prime to p, l is any number $< p+r$ and prime to r, and $\left[\frac{l}{p}\right]_r$ is the least positive root of the congruence $px \equiv l$, mod r.†

2. The residues of $r^{2n}B_{2n}\left(\frac{l}{r}\right)$ and $r^{2n}A'_{2n}\left(\frac{l}{r}\right)$, mod p, where, as before, $p-1$ is a divisor of $2n$, form the subject of the present paper, the principal formulæ giving the residues of

$$r^{p-1}B_{p-1}\left(\frac{l}{r}\right) \text{ and } r^{p-1}A'_{p-1}\left(\frac{l}{r}\right), \text{ mod } p.$$

As in the previous paper, other results are derived from the fundamental formulæ. A quantity $\Omega(r)$ by which the residues are expressed in the case of $l = 1$ is considered at length in §§ 9–44.

Residue of $r^{p-1}B_{p-1}\left(\frac{1}{r}\right)$, mod p. (§§ 3–8.)

3. Let p be any uneven prime and let A_r denote the sum of the products of the numbers 1, 2, ..., $p-1$ taken r together. Then

---

[*] "A Congruence Theorem relating to the Eulerian Numbers and other Coefficients," Vol. xxxii., pp. 171–198.

† *Ib.*, §§ 10, 18 (pp. 174, 178).

evidently

$$x^p+A_1x^{p-1}+A_2x^{p-2}+\ldots+A_{p-2}x^2+A_{p-1}x = x(x+1)(x+2)\ldots(x+p-1).$$

Differentiating with respect to x, we find

$$px^{p-1}+(p-1)\,A_1x^{p-2}+(p-2)\,A_2x^{p-3}+\ldots+2A_{p-2}x+A_{p-1}$$
$$= x\,(x+1)\ldots(x+p-1)\left\{\frac{1}{x}+\frac{1}{x+1}+\ldots+\frac{1}{x+p-1}\right\}. \quad \text{(i.)}$$

Now, $$A_1 = \tfrac{1}{2}p\,(p-1),$$
$$A_{2t+1} \equiv (-1)^{t+1}\frac{(2t+1)\,B_t}{4t}p^2, \quad \text{mod } p^3 \ (t>0),$$
$$A_{2t} \equiv (-1)^t\frac{B_t}{2t}p, \quad \text{mod } p^2,$$

where B_t is the t-th Bernoullian number.*

Thus the left-hand side of (i.)

$$\equiv px^{p-1}+\tfrac{1}{2}px^{p-2}+pB_1x^{p-3}-pB_2x^{p-5}+\ldots+(-1)^{\frac{1}{2}(p-1)}pB_{\frac{1}{2}(p-3)}x^2+A_{p-1},$$
$$\text{mod } p^2,$$

and we therefore find

$$x^{p-1}+\tfrac{1}{2}x^{p-2}+B_1x^{p-3}-B_2x^{p-5}+\ldots+(-1)^{\frac{1}{2}(p-1)}B_{\frac{1}{2}(p-3)}x^2$$
$$\equiv -\frac{(p-1)!}{p}+\frac{x(x+1)\ldots(x+p-1)}{p}\left\{\frac{1}{x}+\frac{1}{x+1}+\ldots+\frac{1}{x+p-1}\right\},$$
$$\text{mod } p. \quad \text{(ii.)}$$

4. Now the Bernoullian function $B_n(x)$, n being even, is defined by the equation†

$$B_n(x) = \frac{x^n}{n}-\tfrac{1}{2}x^{n-1}+\frac{n-1}{2!}B_1x^{n-2}-\frac{(n-1)(n-2)(n-3)}{4!}B_2x^{n-4}+\ldots$$
$$+(-1)^{\frac{1}{2}n}\frac{(n-1)(n-2)\ldots3}{(n-2)!}B_{\frac{1}{2}(n-2)}x^2,$$

and therefore

$$(p-1)\,B_{p-1}(x) = x^{p-1}-\frac{p-1}{2}x^{p-2}+\frac{(p-1)(p-2)}{1.2}B_1x^{p-3}$$
$$-\frac{(p-1)\ldots(p-4)}{4!}B_2x^{p-5}+\ldots+(-1)^{\frac{1}{2}(p-1)}\frac{(p-1)\ldots3}{(p-3)!}B_{\frac{1}{2}(p-3)}x^2,$$
$$\text{mod } p,$$
$$\equiv x^{p-1}+\tfrac{1}{2}x^{p-2}+B_1x^{p-3}-B_2x^{p-5}+\ldots+(-1)^{\frac{1}{2}(p-1)}B_{\frac{1}{2}(p-3)}x^2, \text{ mod } p.$$

---

* *Quarterly Journal*, Vol. xxxi., pp. 326, 327.

† *Proc. Lond. Math. Soc.*, Vol. xxxi., p. 203.

Thus the formula (ii.) shows that

$$(p-1)B_{p-1}(x) \equiv -\frac{(p-1)!}{p} + \frac{x(x+1)\dots(x+p-1)}{p}$$

$$\times \left\{ \frac{1}{x} + \frac{1}{x+1} + \dots + \frac{1}{x+p-1} \right\}, \quad \text{mod } p, \qquad \text{(iii.)}$$

and therefore

$$B_{p-1}(x) \equiv \frac{(p-1)!}{p} - \frac{x(x+1)\dots(x+p-1)}{p}$$

$$\times \left\{ \frac{1}{x} + \frac{1}{x+1} + \dots + \frac{1}{x+p-1} \right\}, \quad \text{mod } p. \qquad \text{(iv.)}$$

5. The formula (iv.) corresponds to the formula

$$B_p(x) - x \equiv \frac{x(x+1)\dots(x+p-1)}{p}, \quad \text{mod } p,$$

of the previous paper.* The method of proof is the same for both formulæ, the investigation in the two preceding sections being similar to that in §§ 2 and 3 of the previous paper.

6. When x is a positive integer, the formula (iv.) may be easily verified. For let $x = kp+t$, where $t<p$; then

$$x(x+1)\dots(x+p-1)$$

$$= (kp+t)(kp+t+1)\dots(kp+p-1)(kp+p)$$

$$\times (kp+p+1)(kp+p+2)\dots(kp+p+t-1)$$

$$\equiv (k+1)p \times t(t+1)\dots(p-1)\left(1+\frac{kp}{t}\right)\left(1+\frac{kp}{t+1}\right)\dots\left(1+\frac{kp}{p-1}\right)$$

$$\times 1.2\dots t\left(1+\frac{kp+p}{1}\right)\left(1+\frac{kp+p}{2}\right)\dots\left(1+\frac{kp+p}{t-1}\right)$$

$$\equiv (k+1)p \times (p-1)!\left(1+\frac{kp}{t}+\frac{kp}{t+1}+\dots+\frac{kp}{p-1}\right.$$

$$\left. +\frac{kp+p}{1}+\frac{kp+p}{2}+\dots+\frac{kp+p}{t-1}\right), \quad \text{mod } p^2$$

$$\equiv (k+1)p \times (p-1)!(1+hp), \quad \text{mod } p^2,$$

---

* Vol. XXXII., p. 172. We may derive (iv.) from this formula by differentiating with respect to x, for, in general,

$$\frac{d}{dx} B_{2n+1}(x) = 2nB_{2n}(x) + (-1)^{n+1}B_n,$$

where
$$h = 1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{t-1},$$

since
$$1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{p-1} \equiv 0, \mod p.$$

Omitting the divisible number $kp+p$, the other $p-1$ numbers in $x, x+1, \ldots, x+p-1$ are $\equiv 1, 2, 3, \ldots, p-1$, mod p, in some order; therefore the sum of their reciprocals $\equiv 0$, mod p, and we have

$$\frac{1}{x}+\frac{1}{x+1}+\ldots+\frac{1}{x+p-1} \equiv \frac{1}{(k+1)p}, \mod p,$$

Thus the formula (iv.) gives in this case

$$B_{p-1}(x) \equiv \frac{(p-1)!}{p} - (k+1)(p-1)!\,(1+hp)\,\frac{1}{(k+1)p}, \mod p,$$
$$\equiv -(p-1)!\,h \equiv h, \mod p,$$

that is,
$$B_{p-1}(kp+t) \equiv 1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{t-1}, \mod p.$$

This result is evidently true, for

$$B_{p-1}(kp+t) = 1^{p-2}+2^{p-2}+3^{p-2}+\ldots+(kp+t-1)^{p-2}$$
$$\equiv 1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{kp+t-1}, \mod p,$$

which
$$\equiv 1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{t-1}, \mod p,$$

since
$$\frac{1}{np+1}+\frac{1}{np+2}+\ldots+\frac{1}{np+p-1} \equiv 0, \mod p.$$

- - - - - - - - - - - - - - - - - -

so that
$$\frac{d}{dx}B_p(x) = (p-1)\,B_{p-1}(x) + (-1)^{\frac{1}{2}(p+1)}B_{\frac{1}{2}(p-1)}.$$

We thus find, by differentiating,

$$-B_{p-1}(x) + (-1)^{\frac{1}{2}(p+1)}B_{\frac{1}{2}(p-1)} - 1 \equiv \frac{d}{dx}\,\frac{x(x+1)\ldots(x+p-1)}{p}, \mod p,$$

and therefore, since

$$(-1)^{\frac{1}{2}(p+1)}B_{\frac{1}{2}(p-1)} - 1 \equiv \frac{(p-1)!}{p}, \mod p \text{ (Vol. XXXII., p. 172)},$$

we have
$$-B_{p-1}(x) + \frac{(p-1)!}{p} \equiv \frac{d}{dx}\,\frac{x(x+1)\ldots(x+p-1)}{p}, \mod p,$$

which is equivalent to (iv.).

7. Now let $x = \frac{1}{r}$, where r is any positive integer prime to p. The formula (iv.) then becomes

$$r^{p-1}B_{p-1}\left(\frac{1}{r}\right) \equiv \frac{(p-1)!}{p}\,r^{p-1} - \frac{(r+1)(2r+1)\dots\{(p-1)r+1\}}{p}$$

$$\times\left\{1+\frac{1}{r+1}+\frac{1}{2r+1}+\dots+\frac{1}{(p-1)r+1}\right\}, \bmod p. \quad \text{(v.)}$$

Of the $p-1$ numbers $r+1$, $2r+1$, ..., $(p-1)r+1$ one is divisible by p, and we know* that

$$\frac{(r+1)(2r+1)\dots\{(p-1)r+1\}}{p} \equiv (\mu_{p-1}+1)(p-1)!\,\{1+\Pi_1(r)\,p\},$$

$$\bmod p^2,$$

where $$\Pi_1(r) = \frac{\mu_1}{2}+\frac{\mu_2}{3}+\dots+\frac{\mu_{p-2}}{p-1},$$

μ_i being the least positive root of the congruence $p\mu_i + i \equiv 0$, mod r.

Consider now the series

$$1+\frac{1}{r+1}+\frac{1}{2r+1}+\dots+\frac{1}{(p-1)r+1};$$

one of the denominators is the divisible number $(\mu_{p-1}+1)\,p$, and, since the others are $\equiv 1, 2, 3, \dots, p-1$, mod p (in some order), the sum of the other terms of the series $\equiv 0$, mod p.

Thus the series $$\equiv \frac{1}{(\mu_{p-1}+1)\,p}, \bmod p.$$

The formula (v.) therefore gives

$$r^{p-1}B_{p-1}\left(\frac{1}{r}\right) \equiv \frac{(p-1)!}{p}\,r^{p-1} - \frac{(p-1)!}{p}\,\{1+\Pi_1(r)\,p\}, \bmod p,$$

$$\equiv (p-1)!\,\frac{r^{p-1}-1}{p} - (p-1)!\,\Pi_1(r), \bmod p.$$

Now $$\frac{r^{p-1}-1}{p} \equiv g_1(r), \bmod p,†$$

where $$g_1(r) = \frac{\mu_1}{1}+\frac{\mu_2}{2}+\dots+\frac{\mu_{p-1}}{p-1},$$

the μ's being as before.

---

* *Messenger of Mathematics*, Vol. xxx., p. 78.

† *Quarterly Journal*, Vol. xxxii., p. 8.

8. Now let
$$\Omega(r) = \Pi_1(r) - g_1(r),$$
so that
$$\Omega(r) = -\frac{\mu_1}{1} + \frac{\mu_1-\mu_2}{2} + \frac{\mu_2-\mu_3}{3} + \dots + \frac{\mu_{p-2}-\mu_{p-1}}{p-1}, \qquad \text{(vi.)}$$
μ_i being the least positive root of the congruence $p\mu_i + i \equiv 0$, mod r.

The formula then is
$$r^{p-1}B_{p-1}\left(\frac{1}{r}\right) \equiv \Omega(r), \quad \text{mod } p. \qquad \text{(vii.)}$$

Since $r^{p-1} \equiv 1$, mod p, we have also
$$B_{p-1}\left(\frac{1}{r}\right) \equiv \Omega(r), \quad \text{mod } p. \qquad \text{(viii.)}$$

The Quantity $\Omega(r)$. (§§ 9–44.)

9. It is interesting now to consider the nature and the methods of calculating the quantity $\Omega(r)$ which, as has just been shown, represents the residue of $B_{p-1}\left(\frac{1}{r}\right)$, mod p. This quantity is defined by the equation (vi.), viz.,
$$\Omega(r) = -\frac{\mu_1}{1} + \frac{\mu_1-\mu_2}{2} + \frac{\mu_2-\mu_3}{3} + \dots + \frac{\mu_{p-2}-\mu_{p-1}}{p-1}.\text{*}$$

To calculate the μ's we first obtain μ_1 from the congruence
$$p\mu_1 + 1 \equiv 0, \quad \text{mod } r;$$
thus μ_1 depends upon the two quantities p and r. Having found μ_1 we can derive $\mu_2, \mu_3, \dots$ from it by reference to r alone, *i.e.*, we continually add μ_1 and subtract r whenever the sum is greater than r or is equal to r. Thus $\mu_i = i\mu_1 - kr$, where kr is the greatest multiple of r contained in $i\mu_1$.

10. As an example, let $p = 11$, $r = 8$. We have $11\mu_1 + 1 = 0$, mod 8, giving $\mu_1 = 5$, and therefore
$$\mu_1 = 5,\ \mu_2 = 2,\ \mu_3 = 7,\ \mu_4 = 4,\ \mu_5 = 1,\ \mu_6 = 6,\ \mu_7 = 3,\ \mu_8 = 0.$$
Thus
$$\begin{aligned}\Omega(8) &= -\tfrac{5}{1}+\tfrac{3}{2}-\tfrac{5}{3}+\tfrac{3}{4}+\tfrac{3}{5}-\tfrac{5}{6}+\tfrac{3}{7}+\tfrac{3}{8}-\tfrac{5}{9}+\tfrac{3}{10}\\ &= -5\left(\tfrac{1}{1}+\tfrac{1}{2}+\tfrac{1}{3}+\dots+\tfrac{1}{10}\right)\\ &\quad +8\left(\tfrac{1}{2}+\tfrac{1}{4}+\tfrac{1}{5}+\tfrac{1}{7}+\tfrac{1}{8}+\tfrac{1}{10}\right)\\ &\equiv 8\left(\tfrac{1}{2}+\tfrac{1}{4}+\tfrac{1}{5}+\tfrac{1}{7}+\tfrac{1}{8}+\tfrac{1}{10}\right), \quad \text{mod } 11\\ &\equiv 3, \quad \text{mod } 11.\end{aligned}$$

---

* As we are concerned only with the residue of $\Omega(r)$ to mod p, we may, if we please, define $\Omega(r)$ by any of the other congruent expressions which are obtained in the subsequent sections.

11. In this example we notice that the numerators of the negative terms are always 5 ($=\mu_1$) and the numerators of the positive terms 3 ($=r-\mu_1$), the sum of 5 and 3 being 8 ($=r$). This must always be the case, for $\mu_i-\mu_{i-1}$ is equal to either μ_1 or $-(r-\mu_1)$, the former if $\mu_i>\mu_{i-1}$ and the latter if $\mu_i<\mu_{i-1}$.

We therefore have in general

$$\Omega(r)\equiv r\left(\frac{1}{d_1}+\frac{1}{d_2}+\frac{1}{d_3}+\dots\right),\quad \text{mod } p,$$

where d_1, d_2, d_3, ... are the denominators of the positive terms. Thus the calculation of $\Omega(r)$ depends upon the determination of the denominators of the positive terms.

12. The sequence of the negative and positive terms is governed by the magnitudes of μ_1, μ_2, ... To determine this sequence, divide r by μ_1, let q_1 be the quotient and r_1 the remainder; then the first q_1 μ's, viz., μ_1, μ_2, ..., μ_{q_1}, are in ascending order of magnitude. Add r to the remainder r_1 and divide again by μ_1; let q_2 be the quotient and r_2 the remainder; then $\mu_{q_1+1}<\mu_{q_1}$, and the next q_2 μ's, viz., μ_{q_1+1}, μ_{q_1+2}, ..., $\mu_{q_1+q_2}$ are in ascending order of magnitude; the next μ, viz., $\mu_{q_1+q_2+1}$, is less than the preceding one, and therefore $\mu_{q_1+q_2+1}$, ..., $\mu_{q_1+q_2+q_3}$ are in ascending order of magnitude; and so on. Finally we come to a quotient q_n for which the remainder is zero. This occurs for $n=\mu_1$, and, as will be shown in § 14, the sum of the quotients, $q_1+q_2+\dots+q_n$, $=r$. The final sequence of ascending μ's, however, ends with $\mu_{q_1+q_2+\dots+q_n-1}=\mu_{r-1}$ instead of with μ_r, for μ_r is not r, but zero.

Thus, supposing $p-1>r$, we have

$$\begin{aligned}&\Omega(r)\\ &\equiv r\left(\frac{1}{q_1+1}+\frac{1}{q_1+q_2+1}+\dots+\frac{1}{q_1+q_2+\dots+q_{n-1}+1}+\frac{1}{q_1+q_2+\dots+q_n}\right.\\ &\quad+\frac{1}{q_1+r+1}+\frac{1}{q_1+q_2+r+1}+\dots\\ &\quad\left.+\frac{1}{q_1+2r+1}+\frac{1}{q_1+q_2+2r+1}+\dots+\dots\ \dots\right),\quad \text{mod } p.\end{aligned}$$

After the denominator $q_1+q_2+\dots+q_n=r$ has been reached, we obtain the succeeding terms by adding r to the n denominators already obtained, then by adding $2r$ to these first n denominators (or

r to the second n denominators), and so on. The series is to be continued so long as the denominators do not surpass $p-1$.

If $p-1<r$, the denominator $q_1+q_2+\dots+q_n$ is not reached; if $p-1=r$, the series ends with this term.*

13. The preceding reasoning is very easily followed in a numerical example. Taking the case of $p=11$, $r=8$, $\mu_1=5$, considered in § 10, we perform the divisions

$$\begin{array}{l}5\;)\;\;8\;(\;1\\ \quad\;\;\underline{\;5\;}\\ 5\;)\;11\;(\;2\\ \quad\;\;\underline{10}\\ 5\;)\;\;9\;(\;1\\ \quad\;\;\underline{\;5\;}\\ 5\;)\;12\;(\;2\\ \quad\;\;\underline{10}\\ 5\;)\;10\;(\;2\end{array}$$

The quotients 1, 2, 1, 2, 2 correspond to the ascending sequences of the cycle of μ's, viz., taking for the moment $\mu_8=8$ instead of 0, $\mu_1, \mu_2, \mu_3, \dots, \mu_8$ are 5, | 2, 7, | 4, | 1, 6, | 3, 8 | ; the vertical bars separate the sequences, which contain 1, 2, 1, 2, 2 numbers respectively. The denominators of the positive terms are the suffixes of the μ's immediately following the bars, viz., they are 2, 4, 5, 7, 9; but, since the last μ, viz., μ_8, is really 0 and not 8, the last sequence is 1, not 2, and the last denominator of the cycle is 8, not 9.

Thus $$\Omega(8) \equiv 8\left(\tfrac{1}{2}+\tfrac{1}{4}+\tfrac{1}{5}+\tfrac{1}{7}+\tfrac{1}{8}+\tfrac{1}{10}\right), \text{ mod } 11,$$

the denominator 10 being obtained by adding 8 to 2.

14. Now $$\begin{aligned} r &= q_1\mu_1+r_1,\\ r+r_1 &= q_2\mu_1+r_2,\\ r+r_2 &= q_3\mu_1+r_3,\\ \dots &\quad \dots \quad \dots\\ r+r_{n-1} &= q_n\mu_1; \end{aligned}$$

whence we have $$\begin{aligned} r &= q_1\mu_1+r_1,\\ 2r &= (q_1+q_2)\,\mu_1+r_2,\\ 3r &= (q_1+q_2+q_3)\,\mu_1+r_3,\\ \dots &\quad \dots \quad \dots \quad \dots\\ nr &= (q_1+q_2+\dots+q_n)\,\mu_1. \end{aligned}$$

---

* In this case $\Omega(r)=1$. (See § 42.)

Now we know that r, $2r$, ..., $(\mu_1-1)\,r$ when divided by μ_1 leave the system of remainders 1, 2, 3, ..., μ_1-1,* and $\mu_1 r$ divided by μ_1 leaves remainder zero. Therefore n must $= \mu_1$, and the last equation shows that $q_1+q_2+\ldots+q_n = r$.

15. Let $K\left(\dfrac{b}{a}\right)$ denote the integer next greater than $\dfrac{b}{a}$ if $\dfrac{b}{a}$ is fractional, and denote $\dfrac{b}{a}$ if $\dfrac{b}{a}$ is integral; then, from § 14,

$$q_1+q_2+\ldots+q_i+1 = K\left(\frac{ir}{\mu_1}\right),$$

unless $i = n = \mu_1$, in which case

$$q_1+q_2+\ldots+q_n = K\left(\frac{nr}{\mu_1}\right) = r.$$

16. If therefore we put, for all positive values of i,

$$\beta_1 = K\left(\frac{ir}{\mu_1}\right),$$

then
$$\Omega(r) \equiv r\left(\frac{1}{\beta_1}+\frac{1}{\beta_2}+\frac{1}{\beta_3}+\ldots\right), \text{ mod } p, \qquad \text{(ix.)}$$

the series being continued so long as the β's do not surpass $p-1$.† The symbol β_i, as just defined, includes denominators greater than r as well as those up to r, for $\beta_{i+r} = \beta_i+r$.

17. Applying this formula to the example in § 13, viz., $p = 11$, $r = 8$, $\mu_1 = 5$, we have

$$\beta_1 = K\left(\tfrac{8}{5}\right) = 2,$$

$$\beta_2 = K\left(\tfrac{16}{5}\right) = 4,$$

$$\beta_3 = K\left(\tfrac{24}{5}\right) = 5,$$

$$\beta_4 = K\left(\tfrac{32}{5}\right) = 7,$$

$$\beta_5 = K\left(\tfrac{40}{5}\right) = 8,$$

giving
$$\Omega(8) \equiv 8\left(\tfrac{1}{2}+\tfrac{1}{4}+\tfrac{1}{5}+\tfrac{1}{7}+\tfrac{1}{8}+\tfrac{1}{10}\right), \text{ mod } 11.$$

---

* μ_1 is necessarily prime to r, since $p\mu_1+1 \equiv 0$, mod r.

† The number of terms is $\lambda-1$, where λ is the least positive root of the congruence $\lambda r \equiv 1$, mod p. (See § 33.)

18. Instead of the numbers μ_i given by the congruence $p\mu_i + i \equiv 0$, mod p, we may use the numbers m_i given by the congruence $pm_i \equiv i$, mod p, m_i being defined as the least positive rooot of this congruence. It can be shown that the m's and μ's are connected by the relation $m_i = \mu_{p-i} + 1$.* The μ's have the values 0, 1, 2, ..., $r-1$; so that the m's have the values 1, 2, 3, ..., r.

Since $\mu_i = m_{p-i} - 1$, we have

$$\Omega(r) = -\frac{m_{p-1}-1}{1} + \frac{m_{p-1}-m_{p-2}}{2} + \frac{m_{p-2}-m_{p-3}}{3} + \dots + \frac{m_2-m_1}{p-1},$$

which, taking the terms in the reverse order,

$$\equiv \frac{m_1-m_2}{1} + \frac{m_2-m_3}{2} + \dots + \frac{m_{p-2}-m_{p-1}}{p-2} + \frac{m_{p-1}-1}{p-1}, \quad \text{mod } p,$$

since $m_p = 1$†; we may therefore take

$$\Omega(r) = \frac{m_1-m_2}{1} + \frac{m_2-m_3}{2} + \dots + \frac{m_{p-1}-m_p}{p-1}, \tag{x.}$$

m_i being the least positive root of $pm_i - i \equiv 0$, mod p.

19. Applying this formula to the same example, viz., $p = 11$, $r = 8$, we determine m_1 from $11m_1 \equiv 1$, mod 8, giving $m_1 = 3$, and therefore $m_2 = 6$, $m_3 = 1$, $m_4 = 4$, $m_5 = 7$, $m_6 = 2$, $m_7 = 5$, $m_8 = 8$, and the formula gives

$$\begin{aligned}\Omega(8) &= -\tfrac{3}{1} + \tfrac{5}{2} - \tfrac{3}{3} - \tfrac{3}{4} + \tfrac{5}{5} - \tfrac{3}{6} - \tfrac{3}{7} + \tfrac{5}{8} - \tfrac{3}{9} + \tfrac{5}{10} \\ &= -3\left(\tfrac{1}{1} + \tfrac{1}{2} + \tfrac{1}{3} + \dots + \tfrac{1}{10}\right) \\ &\quad + 8\left(\tfrac{1}{2} + \tfrac{1}{5} + \tfrac{1}{8} + \tfrac{1}{10}\right) \\ &\equiv 8\left(\tfrac{1}{2} + \tfrac{1}{5} + \tfrac{1}{8} + \tfrac{1}{10}\right), \quad \text{mod } 11.\end{aligned}$$

---

* The m's and μ's are also connected by the relation $m_i + \mu_i = r$, and in addition we have

$$\mu_i + \mu_{p-i} = r-1, \quad m_i + m_{p-i} = r+1$$

(*Quarterly Journal*, Vol. XXXII., pp. 8, 13, 250). These relations may all be established very simply from the definitions. Taking, for example, $m_i = \mu_{p-i} + 1$, we have, from the definitions of m_i and μ_i, $pm_i - i = l_i r$ and $p\mu_{p-i} + p - i = \lambda_{p-i} r$. Now m_i cannot exceed r, and therefore $l_i < p$. Also μ_{p-i} must be $< r$, and therefore $\lambda_{p-i} < p$. By subtraction we have $p(m_i - \mu_{p-i} - 1) = (l_i - \lambda_{p-i})r$. Since r is prime to p, and l_i and λ_{p-i} are both $< p$, we must have $l_i - \lambda_{p-i} = 0$, and therefore $m_i - \mu_{p-i} - 1 = 0$.

† For m_p is the least positive root of the congruence $pm_p \equiv p$, mod r.

20. We see, as in § 10, that in general, by adding

$$m_1\left(\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{p-1}\right)$$

to the expression for $\Omega(r)$ in (x.), we obtain the formula

$$\Omega(r)\equiv r\left(\frac{1}{d_1}+\frac{1}{d_2}+\frac{1}{d_3}+\ldots\right),\quad \text{mod } p,$$

where $d_1, d_2, d_3, \ldots$ are the denominators of the positive terms in (x.).*

21. To determine the denominators of these positive terms we proceed as in § 12, viz., we divide r by m_1, giving quotient q_1 and remainder r_1, we divide $r+r_1$ by m_1, giving quotient q_2 and remainder r_2, and so on. We thus obtain the equations

$$\begin{aligned} r &= q_1 m_1 + r_1, \\ r+r_1 &= q_2 m_1 + r_2, \\ r+r_2 &= q_3 m_1 + r_3, \\ \ldots & \quad \ldots \quad \ldots \\ r+r_{n-1} &= q_n m_1; \end{aligned}$$

whence

$$\begin{aligned} r &= q_1 m_1 + r_1, \\ 2r &= (q_1+q_2)\, m_1 + r_2, \\ 3r &= (q_1+q_2+q_3)\, m_1 + r_3, \\ \ldots & \quad \ldots \quad \ldots \quad \ldots \\ nr &= (q_1+q_2+\ldots+q_n)\, m_1. \end{aligned}$$

As before, we can prove that $n = m_1$ and $q_1+q_2+\ldots+q_n = r$.

22. In the case of the m's the denominators corresponding to the same suffixes in the numerators are less by unity than in the case of the μ's, so that, corresponding to the formula in § 12, we have

$$\begin{aligned} \Omega(r)\equiv r\Bigg(&\frac{1}{q_1}+\frac{1}{q_1+q_2}+\frac{1}{q_1+q_2+q_3}+\ldots+\frac{1}{q_1+q_2+\ldots+q_n} \\ &+\frac{1}{q_1+r}+\frac{1}{q_1+q_2+r}+\ldots \\ &+\frac{1}{q_1+2r}+\frac{1}{q_1+q_2+2r}+\ldots+\ldots\ldots\Bigg),\quad \text{mod } p. \end{aligned}$$

---

* It will be shown in § 39 that the last denominator is always $p-1$.

23. Let $I\left(\frac{b}{a}\right)$ denote the integer next less than $\frac{b}{a}$ if $\frac{b}{a}$ is fractional, and denote $\frac{b}{a}$ if $\frac{b}{a}$ is integral.*

Then, for all values of i,

$$q_1+q_2+\ldots+q_i = I\left(\frac{ir}{m_1}\right).$$

24. If therefore we put $\quad a_i = I\left(\frac{ir}{m_1}\right),$

we have
$$\Omega(r) \equiv r\left(\frac{1}{a_1}+\frac{1}{a_2}+\frac{1}{a_3}+\ldots\right), \text{ mod } p, \qquad \text{(xi.)}$$

the series being continued so long as the a's do not surpass $p-1$.†

25. Taking the example of § 19 in which $p = 11$, $r = 8$, $m_1 = 3$, the divisions are

$$\begin{array}{r}
3\;)\;\;8\;(\;2 \\
\underline{6}\;\;\;\;\; \\
3\;)\;10\;(\;3 \\
\underline{9}\;\;\;\;\; \\
3\;)\;\;9\;(\;3
\end{array}$$

giving
$$\Omega(8) \equiv 8\left(\tfrac{1}{2}+\tfrac{1}{5}+\tfrac{1}{8}+\tfrac{1}{10}\right), \text{ mod } 11.$$

Using the formula (xi.) of § 24,

$$a_1 = I\left(\tfrac{8}{3}\right) = 2,$$

$$a_2 = I\left(\tfrac{16}{3}\right) = 5,$$

$$a_3 = I\left(\tfrac{24}{3}\right) = 8,$$

giving
$$\Omega(8) \equiv 8\left(\tfrac{1}{2}+\tfrac{1}{5}+\tfrac{1}{8}+\tfrac{1}{10}\right), \text{ mod } 11,$$

as before.

---

[*] Thus $K\left(\frac{b}{a}\right) = 1+I\left(\frac{b}{a}\right)$ when $\frac{b}{a}$ is fractional, and $K\left(\frac{b}{a}\right) = I\left(\frac{b}{a}\right) = \frac{b}{a}$ when $\frac{b}{a}$ is integral.

[†] The number of terms is l, where l is the least positive root of the congruence $lr+1 \equiv 0$, mod p. (See § 39.)

26. The formulæ for $\Omega(r)$ which have been obtained in §§ 24 and 16 are:

$$\Omega(r) \equiv r\left(\frac{1}{a_1}+\frac{1}{a_2}+\frac{1}{a_3}+\dots\right), \bmod p, \qquad \text{(xi.)}$$

where
$$pm_1 \equiv 1, \bmod r,$$
$$a_i = I\left(\frac{ir}{m_1}\right);$$

and
$$\Omega(r) \equiv r\left(\frac{1}{\beta_1}+\frac{1}{\beta_2}+\frac{1}{\beta_3}+\dots\right), \bmod p, \qquad \text{(ix.)}$$

where
$$p\mu_1 \equiv -1, \bmod r,$$
$$\beta_i = K\left(\frac{ir}{\mu_1}\right).$$

The most convenient method of determining $\Omega(r)$ is therefore as follows.

From p and r we form the congruence $pm_1 \equiv 1, \bmod r$, and therefrom determine m_1; if $m_1 < \frac{1}{2}r$, we retain m_1 and use the formula (xi.), *i.e.*, we form the values of $a_i = I\left(\frac{ir}{m_1}\right)$, but, if $m_1 > \frac{1}{2}r$, we derive $\mu_1 = r - m_1$ from m_1, and use the formula (ix.), *i.e.*, we form the values of $\beta_i = K\left(\frac{ir}{\mu_1}\right)$.

27. As examples, (i.) let $p = 13$, $r = 9$. We find m_1 from

$$13m_1 \equiv 1, \bmod 9,$$

Thus $m_1 = 7$, which $> \frac{1}{2}r$. We therefore take $\mu_1 = 9 - 7 = 2$, and calculate
$$\beta_1 = K\left(\tfrac{9}{2}\right) = 5, \quad \beta_2 = K\left(\tfrac{18}{2}\right) = 9;$$

whence
$$\Omega(9) \equiv 9\left(\tfrac{1}{5}+\tfrac{1}{9}\right), \bmod 13.$$

(ii.) Let $p = 17$, $r = 10$. We find m_1 from $17m_1 \equiv 1, \bmod 10$; therefore $m_1 = 3$, which we retain, since it $< \frac{1}{2}r$, and calculate

$$a_1 = I\left(\tfrac{10}{3}\right) = 3, \quad a_2 = I\left(\tfrac{20}{3}\right) = 6, \quad a_3 = I\left(\tfrac{30}{3}\right) = 10;$$

whence
$$\Omega(10) \equiv 10\left(\tfrac{1}{3}+\tfrac{1}{6}+\tfrac{1}{10}+\tfrac{1}{13}+\tfrac{1}{16}\right), \bmod 17.$$

28. Two other forms for $\Omega(r)$ should also be noticed.

In the original formula (vi.) of § 9, viz.,

$$\Omega(r) = -\frac{\mu_1}{1} + \frac{\mu_1-\mu_2}{2} + \frac{\mu_2-\mu_3}{3} + \ldots + \frac{\mu_{p-2}-\mu_{p-1}}{p-1},$$

substitute $r-1-\mu_{p-i}$ for μ_i throughout (§ 18, note). We thus find

$$\Omega(r) = -(r-1) + \frac{\mu_{p-1}}{1} + \frac{\mu_{p-2}-\mu_{p-1}}{2} + \ldots + \frac{\mu_1-\mu_2}{p-1}, \text{ mod } p. \tag{xii.}$$

Substituting $-(p-i)$ for i in the denominators, replacing $r-1$ by μ_p,* and changing the signs of the terms throughout, we find

$$-\Omega(r) \equiv \frac{\mu_1-\mu_2}{1} + \frac{\mu_2-\mu_3}{2} + \ldots + \frac{\mu_{p-2}-\mu_{p-1}}{p-2} + \frac{\mu_{p-1}-\mu_p}{p-1}, \text{ mod } p.$$

Now $\mu_{p-1}-\mu_p = -\mu_1$, for $\mu_p = r-1$, and therefore μ_{p-1} must necessarily be $<\mu_p$; so that we have

$$-\Omega(r) \equiv \frac{\mu_1-\mu_2}{1} + \frac{\mu_2-\mu_3}{2} + \ldots + \frac{\mu_{p-2}-\mu_{p-1}}{p-2} - \frac{\mu_1}{p-1}, \text{ mod } p.$$

29. In this expression for $-\Omega(r)$ the terms $\frac{\mu_1-\mu_2}{1}, \ldots, \frac{\mu_{p-2}-\mu_{p-1}}{p-2}$ differ from the terms $\frac{\mu_1-\mu_2}{2}, \ldots, \frac{\mu_{p-2}-\mu_{p-1}}{p-1}$ in the original expression (vi.) for $\Omega(r)$ only in having the denominators diminished by unity (the signs of the terms and the numerators being unaltered); and, in place of the first term $-\frac{\mu_1}{1}$, we have the term $-\frac{\mu_1}{p-1}$.

Thus when we add, as in §§ 10 and 11, the expression

$$\mu_1\left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1}\right),$$

which $\equiv 0$, mod p, we are left with exactly the same positive terms, except that their denominators are diminished by unity; *i.e.*, using the notation of § 11, we have

$$-\Omega(r) \equiv r\left(\frac{1}{d_1-1} + \frac{1}{d_2-1} + \frac{1}{d_3-1} + \ldots\right), \text{ mod } p,$$

$d_1, d_2, d_3, \ldots$ being the denominators of the positive terms in the original formula (vi.) for $\Omega(r)$.

---

* μ_p is the least positive root of $p\mu_p + p \equiv 0$, mod r; therefore $p\mu_p + p = ar$, where, since $\mu_p < r$, a must be $= p$, and therefore $\mu_p = r-1$.

30. Thus, taking the example in § 10, the original formula for $\Omega(r)$ gave

$$-\tfrac{5}{1}+\tfrac{3}{2}-\tfrac{5}{3}+\tfrac{3}{4}+\tfrac{3}{5}-\tfrac{5}{6}+\tfrac{3}{7}+\tfrac{3}{8}-\tfrac{5}{9}+\tfrac{3}{10},$$

and the above formula for $-\Omega(r)$ gives

$$\tfrac{3}{1}-\tfrac{5}{2}+\tfrac{3}{3}+\tfrac{3}{4}-\tfrac{5}{5}+\tfrac{3}{6}+\tfrac{3}{7}-\tfrac{5}{8}+\tfrac{3}{9}-\tfrac{5}{10}.$$

By adding $$5\left(\tfrac{1}{1}+\tfrac{1}{2}+\ldots+\tfrac{1}{10}\right),$$

we obtain from the first expression, as in § 10,

$$\Omega(8) \equiv 8\left(\tfrac{1}{2}+\tfrac{1}{4}+\tfrac{1}{5}+\tfrac{1}{7}+\tfrac{1}{8}+\tfrac{1}{10}\right), \quad \text{mod } 11,$$

and from the second

$$-\Omega(8) \equiv 8\left(\tfrac{1}{1}+\tfrac{1}{3}+\tfrac{1}{4}+\tfrac{1}{6}+\tfrac{1}{7}+\tfrac{1}{9}\right), \quad \text{mod } 11.$$

31. If therefore we denote by $I'\left(\frac{b}{a}\right)$ the integer next less than $\frac{b}{a}$, whether $\frac{b}{a}$ be fractional or integral,* and if we put, for all values of i,

$$\gamma_i = I'\left(\frac{ir}{\mu_1}\right),$$

then we have

$$\Omega(r) \equiv -r\left(\frac{1}{\gamma_1}+\frac{1}{\gamma_2}+\frac{1}{\gamma_3}+\ldots\right), \quad \text{mod } p, \qquad \text{(xiii.)}$$

the series being continued so long as the denominators do not surpass $p-1$.

32. This formula may be connected directly with the formula (ix.) (§ 26) as follows.

We have $$\beta_i = K\left(\frac{ir}{\mu_1}\right), \quad \gamma_i = I'\left(\frac{ir}{\mu_1}\right),$$

and it can be shown that, if $\lambda = \frac{p\mu_1+1}{r}$, then

$$\beta_i + \gamma_{\lambda-i} = p.$$

---

* $I'\left(\frac{b}{a}\right)$ is the same as $I\left(\frac{b}{a}\right)$ when $\frac{b}{a}$ is fractional, and $= I\left(\frac{b}{a}\right)-1$ when $\frac{b}{a}$ is integral.

For let $\frac{ir}{\mu_1} = h + \frac{\epsilon}{\mu_1}$, h being an integer and $\epsilon < \mu_1$; then

$$\beta_i = K\left(h + \frac{\epsilon}{\mu_1}\right), \quad \gamma_{\lambda-i} = I'\left(p - h + \frac{1-\epsilon}{\mu_1}\right);$$

and therefore,

$$\begin{array}{lll} \text{(i.) if } \epsilon > 1, & \beta_i = h+1, & \gamma_{\lambda-i} = p-h-1; \\ \text{(ii.) if } \epsilon = 1, & \beta_i = h+1, & \gamma_{\lambda-i} = p-h-1; \\ \text{(iii.) if } \epsilon = 0, & \beta_i = h, & \gamma_{\lambda-i} = p-h; \end{array}$$

so that in all three cases $\beta_i + \gamma_{\lambda-i} = p$.

33. Now in the formula (ix.), viz.,

$$\Omega(r) \equiv r\left(\frac{1}{\beta_1} + \frac{1}{\beta_2} + \frac{1}{\beta_3} + \dots\right), \quad \text{mod } p,$$

the last numerator is $\beta_{\lambda-1}$, for

$$\beta_\lambda = K\left(\frac{\lambda r}{\mu_1}\right) = K\left(p + \frac{1}{\mu_1}\right) = p+1,$$

which $> p-1$.

Also $$\beta_{\lambda-1} = K\left(\frac{\lambda r - r}{\mu_1}\right) = K\left(p - \frac{r-1}{\mu_1}\right),$$

which, since $\mu_1 < r$, must be $<$ or $= p-1$.

Thus, in (ix.), the denominators are $\beta_1, \beta_2, \dots, \beta_{\lambda-1}$; and therefore the corresponding γ's derived from them are $\gamma_{\lambda-1}, \gamma_{\lambda-2}, \dots, \gamma_1$. The number of the γ's in (xiii.) is therefore $\lambda - 1$, and, since $\beta_i + \gamma_{\lambda-i} = p$ and β_1 cannot be <2, the largest γ, viz., $\gamma_{\lambda-1}$, cannot exceed $p-2$.

34. Since $\gamma_i = \beta_i - 1$ for all values of i, we have thus proved the relations

$$\beta_i + \beta_{\lambda-i} = p+1,$$

$$\gamma_i + \gamma_{\lambda-i} = p-1,$$

where $$\lambda = \frac{p\mu_1 + 1}{r}.$$

Assuming that we know that, in the formula (ix.), the β's run from β_1 to $\beta_{\lambda-1}$, the first of these relations shows at once why in that formula we may diminish all the denominators by unity if at the same time we change the sign of $\Omega(r)$.

These relations show also that the sum of any pair of denominators which are equidistant from the beginning and end of the series in (ix.) is $p+1$, and in (xiii.) is $p-1$. When λ is even, there is a middle term whose denominator $\beta_{\frac{1}{2}\lambda}$ or $\gamma_{\frac{1}{2}\lambda}$ is equal to $\frac{1}{2}(p+1)$ or $\frac{1}{2}(p-1)$ respectively.

The number λ is the least positive root of the congruence

$$\lambda r \equiv 1, \quad \text{mod } p.$$

35. Treating in the same manner as in § 29 the formula (x.) of § 18, viz.,

$$\Omega(r) = \frac{m_1-m_2}{1} + \frac{m_2-m_3}{2} + \ldots + \frac{m_{p-1}-m_p}{p-1},$$

we substitute $r+1-m_{p-i}$ for m_i throughout, we put $-(p-i)$ for i in the denominators, and change the signs of all the terms. We thus find

$$-\Omega(r) \equiv \frac{r-m_1}{1} + \frac{m_1-m_2}{2} + \ldots + \frac{m_{p-2}-m_{p-1}}{p-1}, \quad \text{mod } p.$$

The terms $\frac{m_1-m_2}{2}, \ldots, \frac{m_{p-2}-m_{p-1}}{p-1}$ differ from the first $p-2$ terms of (x.) only by an increase of unity in the denominators. The only other change is that we have the new term $\frac{r-m_1}{1}$ in place of the last term $\frac{m_{p-1}-m_p}{p-1}$ which $= \frac{r-m_1}{p-1}$.

Thus, when we add

$$m_1\left(\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{p-1}\right),$$

the resulting expression differs from that in § 20 only by the substitution of $\frac{r}{1}$ for $\frac{r}{p-1}$, and the increase of the other denominators by unity.

36. Taking the example of § 19, the expression for $\Omega(8)$ found in that section was

$$\Omega(8) \equiv -\tfrac{3}{1}+\tfrac{5}{2}-\tfrac{3}{3}-\tfrac{3}{4}+\tfrac{5}{5}-\tfrac{3}{6}-\tfrac{3}{7}+\tfrac{5}{8}-\tfrac{3}{9}+\tfrac{5}{10}, \quad \text{mod } 11,$$

while the formula (xiv.) gives

$$-\Omega(8) \equiv \tfrac{5}{1}-\tfrac{3}{2}+\tfrac{5}{3}-\tfrac{3}{4}-\tfrac{3}{5}+\tfrac{5}{6}-\tfrac{3}{7}-\tfrac{3}{8}+\tfrac{5}{9}-\tfrac{3}{10}, \quad \text{mod } 11.$$

Adding $$3\left(\tfrac{1}{1}+\tfrac{1}{2}+\tfrac{1}{3}+\ldots+\tfrac{1}{10}\right),$$
the formulæ become

$$\Omega(8) \equiv 8\left(\tfrac{1}{2}+\tfrac{1}{5}+\tfrac{1}{8}+\tfrac{1}{10}\right), \quad \text{mod } 11,$$

$$-\Omega(8) \equiv 8\left(\tfrac{1}{1}+\tfrac{1}{3}+\tfrac{1}{6}+\tfrac{1}{10}\right), \quad \text{mod } 11,$$

respectively.

37. If therefore we denote by $K'\left(\frac{b}{a}\right)$ the integer next greater than $\frac{b}{a}$ whether $\frac{b}{a}$ be fractional or integral,* and if we put

$$\delta_i = K'\left(\frac{ir}{m_1}\right),$$

then we have $$\Omega(r) \equiv -r\left(1+\frac{1}{\delta_1}+\frac{1}{\delta_2}+\ldots\right), \quad \text{mod } p; \qquad \text{(xv.)}$$

the series being continued so long as the denominators do not surpass $p-1$.

38. To connect the formulæ directly with (xi.), we have

$$a_i = I\left(\frac{ir}{m_1}\right), \quad \delta_i = K'\left(\frac{ir}{m_1}\right),$$

and we can show that, if $l = \frac{pm_1-1}{r}$, then

$$a_i + \delta_{l-i} = p.$$

For let $$\frac{ir}{m_1} = h + \frac{\epsilon}{m_1},$$

h being an integer and $\epsilon < m_1$; then

$$a_i = I\left(h+\frac{\epsilon}{m_1}\right), \quad \delta_{l-i} = K'\left(p-h-\frac{1+\epsilon}{m_1}\right).$$

Thus $$a_i = h \text{ and } \delta_{l-i} = p-h;$$

so that $$a_i + \delta_{l-i} = p.$$

---

* $K'\left(\frac{b}{a}\right)$ is the same as $K\left(\frac{b}{a}\right)$ when $\frac{b}{a}$ is fractional, and $= K\left(\frac{b}{a}\right)+1$ when $\frac{b}{a}$ is integral.

39. Now, in the formula (xi.), the last denominator is a_l, and its value is $p-1$, for

$$a_l = I\left(\frac{lr}{m_1}\right) = I\left(p-\frac{1}{m_1}\right) = p-1.$$

Thus in (xi.) the denominators are l in number, and the last denominator $a_l = p-1$. The corresponding δ's are $\delta_{l-1}, \delta_{l-2}, \ldots, \delta_0$. To determine δ_0 we have the equation $a_l+\delta_0 = p$, that is, $p-1+\delta_0 = p$; so that $a_0 = 1$, and we therefore obtain the formula

$$\Omega(r) \equiv -r\left(\frac{1}{1}+\frac{1}{\delta_1}+\frac{1}{\delta_2}+\ldots+\frac{1}{\delta_{l-1}}\right), \text{ mod } p.$$

40. Since $\delta_i = a_i+1$, we deduce from $a_i+\delta_{l-i} = p$ the relations

$$a_i+a_{l-i} = p-1,$$
$$\delta_i+\delta_{l-i} = p+1,$$

in the first of which we suppose that a_0, which does not occur in the formula (xi.), is zero. In the second relation δ_0, which does occur in the formula (xv.), is unity.

We thus see that, leaving out of consideration the last denominator $p-1$ in (xi.), the sum of any pair of denominators equidistant from the beginning and end of the series is $p-1$. When l is even there is a middle term whose denominator a_μ is $\frac{1}{2}(p-1)$.

Similarly, in (xv.), leaving out of consideration the first term 1, the sum of any pair of equidistant denominators is $p+1$. When l is even, there is a middle term whose denominator δ_μ is $\frac{1}{2}(p+1)$.

The number l is the least positive root of the congruence

$$lr+1 \equiv 0, \text{ mod } p.$$

41. As another example of the formulæ (xi.) and (ix.) (§ 26), (xiii.) (§ 31), (xv.) (§ 37), we may take $p = 13$, $r = 5$; so that $m_1 = 2$, $\mu_1 = 3$.

Here $a_1 = I(\frac{5}{2}) = 2, \quad a_2 = I(\frac{10}{2}) = 5$;

so that (xi.) gives

$$\Omega(5) \equiv 5\left(\tfrac{1}{2}+\tfrac{1}{5}+\tfrac{1}{7}+\tfrac{1}{10}+\tfrac{1}{12}\right), \text{ mod } 13,$$

and $\beta_1 = K(\frac{5}{3}) = 2, \quad \beta_2 = K(\frac{10}{3}) = 4, \quad \beta_3 = K(\frac{15}{3}) = 5$;

so that (ix.) gives

$$\Omega(5) \equiv 5\left(\tfrac{1}{2}+\tfrac{1}{4}+\tfrac{1}{5}+\tfrac{1}{7}+\tfrac{1}{9}+\tfrac{1}{10}+\tfrac{1}{12}\right), \text{ mod } 13.$$

Also $$\gamma_1 = 1, \quad \gamma_2 = 3, \quad \gamma_3 = 4;$$
so that (xiii.) gives
$$\Omega(5) \equiv -5\left(\tfrac{1}{1}+\tfrac{1}{3}+\tfrac{1}{4}+\tfrac{1}{6}+\tfrac{1}{8}+\tfrac{1}{9}+\tfrac{1}{11}\right), \quad \text{mod } 13,$$
and $$\delta_1 = 3;$$
so that (xv.) gives
$$\Omega(5) \equiv -5\left(\tfrac{1}{1}+\tfrac{1}{3}+\tfrac{1}{6}+\tfrac{1}{8}+\tfrac{1}{11}\right), \quad \text{mod } 13.$$
Each formula when reduced gives $\Omega(5) \equiv 9$, mod 13.

42. The expression for $\Omega(r)$ assumes a very simple form when $m_1 = 1$, that is, when $p = kr+1$; and when $\mu_1 = 1$, that is, when $p = kr+r-1$.

If $p = kr+1$, then $m_1 = 1$, and therefore $a_1 = I(r) = r$; so that
$$\Omega(r) \equiv r\left(\frac{1}{r}+\frac{1}{2r}+\frac{1}{3r}+\dots+\frac{1}{kr}\right), \quad \text{mod } p,$$
$$\equiv 1+\frac{1}{2}+\frac{1}{3}+\dots+\frac{1}{k}, \quad \text{mod } p.$$
If $p = kr+r-1$, then $\mu_1 = 1$, and therefore $\beta_1 = K(r) = r$; so that
$$\Omega(r) \equiv r\left(\frac{1}{r}+\frac{1}{2r}+\frac{1}{3r}+\dots+\frac{1}{kr}\right), \quad \text{mod } p,$$
$$\equiv 1+\frac{1}{2}+\frac{1}{3}+\dots+\frac{1}{k}, \quad \text{mod } p.$$

43. Since every prime is of the forms $2k+1$, $3k+1$ or $3k+2$, $4k+1$ or $4k+3$, $6k+1$ or $6k+5$, these formulæ show that, $I\left(\frac{b}{a}\right)$ denoting the greatest integer contained in $\frac{b}{a}$,
$$\Omega(2) \equiv 1+\frac{1}{2}+\dots+\frac{1}{k}. \quad \text{mod } p, \quad \text{where } k = I\left(\frac{p}{2}\right);$$
$$\Omega(3) \equiv 1+\frac{1}{2}+\dots+\frac{1}{k}, \quad \text{mod } p, \quad \text{where } k = I\left(\frac{p}{3}\right);$$
$$\Omega(4) \equiv 1+\frac{1}{2}+\dots+\frac{1}{k}, \quad \text{mod } p, \quad \text{where } k = I\left(\frac{p}{4}\right);$$
$$\Omega(6) \equiv 1+\frac{1}{2}+\dots+\frac{1}{k}, \quad \text{mod } p, \quad \text{where } k = I\left(\frac{p}{6}\right).$$

44. The function Ω satisfies the following curious relation :

$$\Omega(p-r) \equiv \Omega(r)+r, \quad \text{mod } p.$$

To prove this formula let m_i and m'_i denote respectively the least positive roots of the congruences

$$pm_i \equiv i, \quad \text{mod } r,$$

$$pm'_i \equiv i, \quad \text{mod } p-r.$$

Then we have

$$pm_i = i+l_i r,$$

$$pm'_i = i+l'_i\,(p-r),$$

where l_i and l'_i must be $< p$.

Subtracting, we find

$$p\,(m_i-m'_i) = (l_i+l'_i)\,r-l'_i\,p.$$

Since r is prime to p, and l_i and l'_i are both $<p$, we must have $l_i+l'_i = p$. Thus the original equations may be written

$$pm_i = i+l_i r,$$

$$pm'_i = i+(p-l_i)(p-r).$$

Equating the values of l_i given by these two equations, we have

$$\frac{pm_i-i}{r} = \frac{pm'_i-i-p\,(p-r)}{r-p},$$

giving

$$m_i \equiv m'_i+r-\frac{i}{r}, \quad \text{mod } p.$$

Substituting for the m's from this formula in the formula (x.) of § 18, viz.,

$$\Omega(r) \equiv \frac{m_1-m_2}{1}+\frac{m_2-m_3}{2}+\dots+\frac{m_{p-2}-m_{p-1}}{p-2}+\frac{m_{p-1}-1}{p-1}, \quad \text{mod } p,$$

we find

$$\Omega(r) \equiv \left(\frac{m'_1-m'_2}{1}+\frac{1}{r}\right)+\left(\frac{m'_2-m'_3}{2}+\frac{1}{2r}\right)+\dots$$

$$+\left(\frac{m'_{p-2}-m'_{p-1}}{p-2}+\frac{1}{(p-2)\,r}\right)+\left(\frac{m'_{p-1}-1}{p-1}+\frac{r}{p-1}-\frac{1}{r}\right), \text{ mod } p,$$

$$\equiv \Omega(p-r)-r, \quad \text{mod } p.^{*}$$

---

[*] It can also be shown that

$$\Omega(p+r) \equiv \Omega(r), \text{ mod } p \quad (\S\ 52).$$

Residues of $r^{2n}B_{2n}\left(\frac{1}{r}\right)$ *and of the series involving Bernoullian Numbers derived therefrom.* (§§ 45–52.)

45. Since
$$B_n(x) \equiv B_{n-k(p-1)}(x), \quad \text{mod } p,\text{*}$$
we have
$$r^{k(p-1)+p-1}B_{k(p-1)+p-1}(x) \equiv r^{p-1}B_{p-1}(x), \quad \text{mod } p;$$
and therefore, putting $x = \frac{1}{r}$,
$$r^{k(p-1)+p-1}B_{k(p-1)+p-1}\left(\frac{1}{r}\right) \equiv r^{p-1}B_{p-1}\left(\frac{1}{r}\right), \quad \text{mod } p,$$
$$\equiv \Omega(r), \quad \text{mod } p.$$

If therefore p is any uneven prime, such that $p-1$ is a divisor of $2n$ (*i.e.*, if p is any uneven Staudt factor for n), then
$$r^{2n}B_{2n}\left(\frac{1}{r}\right) \equiv \Omega(r), \quad \text{mod } p. \qquad \text{(xvii.)}$$

46. In the case of $r^{2n+1}B_{2n+1}\left(\frac{1}{r}\right)$ discussed in the previous paper, the particular values $r = 4, 3, 6$ gave the Eulerian numbers, and the numbers I_n and J_n† ; but in the present case of $r^{2n}B_{2n}\left(\frac{1}{r}\right)$ we only obtain quantities involving Bernoullian numbers by assigning to r the values $r = 2, 3, 4, 6$; viz., the formulæ are‡

$$2^{2n}B_{2n}(\tfrac{1}{2}) = (-1)^n(2^{2n}-1)\frac{B_n}{n}, \qquad (1)$$

$$3^{2n}B_{2n}(\tfrac{1}{3}) = (-1)^n(3^{2n+1}-3)\frac{B_n}{4n}, \qquad (2)$$

$$4^{2n}B_{2n}(\tfrac{1}{4}) = (-1)^n(2^{4n-1}+2^{2n-1}-1)\frac{B_n}{n}, \qquad (3)$$

$$6^{2n}B_{2n}(\tfrac{1}{6}) = (-1)^n(6^{2n}+2.3^{2n}+3.2^{2n}-6)\frac{B_n}{4n}. \qquad (4)$$

---

* *Proc. Lond. Math. Soc.*, Vol. XXXI., p. 206.
† *Ibid.*, Vol. XXXII., p. 175.
‡ *Quarterly Journal*, Vol. XXIX., pp. 26, 31, 36, 42.

47. The residues given by the general formula of § 45 may be easily verified in the case of (1) and (2).

In the case of (1), putting $2n = p-1$, the formula gives

$$(-1)^{\frac{1}{2}(p-1)}(2^{p-1}-1)\frac{B_{\frac{1}{2}(p-1)}}{\frac{1}{2}(p-1)} \equiv \Omega(r), \mod p.$$

The left-hand side $\equiv (-1)^{\frac{1}{2}(p+1)} 2 (2^{p-1}-1) B_{\frac{1}{2}(p-1)}$, mod p,

and, from Staudt's theorem,

$$pB_{\frac{1}{2}(p-1)} \equiv (-1)^{\frac{1}{2}(p-1)}, \mod p;$$

so that the congruence reduces to

$$-2\frac{2^{p-1}-1}{p} \equiv \Omega(2), \mod p.$$

If $p = 2k+1$,

$$\frac{2^{p-1}-1}{p} \equiv 1+\frac{1}{3}+\frac{1}{5}+\ldots+\frac{1}{p-2}, \mod p,\text{*}$$

$$\equiv -\frac{1}{2}-\frac{1}{4}-\frac{1}{6}-\ldots-\frac{1}{2k} \equiv -\frac{1}{2}\left(1+\frac{1}{2}+\ldots+\frac{1}{k}\right), \mod p,$$

and, from § 43, $\Omega(r) \equiv 1+\frac{1}{2}+\ldots+\frac{1}{k}$, mod p;

so that the congruence is verified.

48. In the case of (2), putting $2n = p-1$, the formula (xvi.) of § 45 gives

$$(-1)^{\frac{1}{2}(p-1)}\tfrac{3}{4}(3^{p-1}-1)\frac{B_{\frac{1}{2}(p-1)}}{\frac{1}{2}(p-1)} \equiv \Omega(3), \mod p,$$

which reduces to $-\frac{3}{2}\frac{3^{p-1}-1}{p} \equiv \Omega(3)$, mod p.

If $p = 3k+1$, then $\mu_1 = 2$, and

$$\frac{3^{p-1}-1}{p} \equiv \frac{2}{1}+\frac{1}{2}+\frac{0}{3}+\ldots+\frac{2}{3k-2}+\frac{1}{3k-1}+\frac{0}{3k}, \mod p,$$

$$\equiv \frac{1}{1}-\frac{1}{3}+\frac{1}{4}-\frac{1}{6}+\ldots+\frac{1}{3k-2}-\frac{1}{3k}, \mod p.$$

---

* *Quarterly Journal*, Vol. xxxii., p. 21.

Replacing $\frac{1}{1}, \frac{1}{4}, \frac{1}{7}, \ldots, \frac{1}{3k-2}$ by $-\frac{1}{p-1}, -\frac{1}{p-4}, \ldots, -\frac{1}{3}$, that is, by $-\frac{1}{3k}, -\frac{1}{3k-3}, \ldots, -\frac{1}{3}$, we have

$$\frac{3^{p-1}-1}{p} \equiv -\frac{2}{3}-\frac{2}{6}-\ldots-\frac{2}{3k}, \mod p,$$

$$\equiv -\frac{2}{3}\left(1+\frac{1}{2}+\ldots+\frac{1}{k}\right), \mod p;$$

and therefore, since

$$\Omega(3) \equiv 1+\frac{1}{2}+\ldots+\frac{1}{k}, \mod p \ (\S\ 43),$$

the theorem is verified when $p = 3k+1$.

If $p = 3k+2$, then $\mu_1 = 1$, and

$$\frac{3^{p-1}-1}{p} \equiv \frac{1}{1}+\frac{2}{2}+\frac{0}{3}+\ldots+\frac{1}{3k-2}+\frac{2}{3k-1}+\frac{0}{3k}, \mod p,$$

$$\equiv \frac{1}{2}-\frac{1}{3}+\frac{1}{5}-\frac{1}{6}+\ldots+\frac{1}{3k-1}-\frac{1}{3k},$$

which $$\equiv -\frac{2}{3}\left(1+\frac{1}{2}+\ldots+\frac{1}{k}\right), \mod p.$$

From § 43, $$\Omega(3) \equiv 1+\frac{1}{2}+\ldots+\frac{1}{k}, \mod p;$$

and therefore the theorem is verified also for $p = 3k+2$.

49. It was shown in § 4 that

$$B_{p-1}(x) \equiv x^{p-1}-\tfrac{1}{2}x^{p-2}-B_1x^{p-3}+B_2x^{p-5}-\ldots+(-1)^{\frac{1}{2}(p-3)}B_{\frac{1}{2}(p-3)}x^2, \mod p.$$

When x is a positive integer, we have (§ 6)

$$B_{p-1}(x) \equiv \frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{x-1}, \mod p;$$

and therefore in this case

$$x^{p-3}B_1-x^{p-5}B_2+\ldots+(-1)^{\frac{1}{2}(p-1)}x^2B_{\frac{1}{2}(p-3)} \equiv -1-\frac{1}{2x}-B_{p-1}(x), \mod p,$$

$$\equiv -1-\frac{1}{2x}-\frac{1}{1}-\frac{1}{2}-\frac{1}{3}-\ldots-\frac{1}{x-1}, \mod p.$$

50. This formula connects the residues, mod p, of the first $\frac{1}{2}(p-3)$ Bernoullian numbers, and involves an arbitrary integer x. The powers of the integer decrease as the suffixes of the Bernoullian numbers increase. We may, however, obtain a more interesting formula in which the powers increase with the suffixes by putting $x = \dfrac{1}{r}$. We thus find

$$r^{p-1}B_{p-1}\left(\frac{1}{r}\right) \equiv -1-\tfrac{1}{2}r-B_1r^2+B_2r^4-\ldots+(-1)^{\frac{1}{2}(p-3)}B_{\frac{1}{2}(p-3)}r^{p-3}, \quad \text{mod } p\,;$$

and therefore, since

$$r^{p-1}B_{p-1}\left(\frac{1}{r}\right) \equiv \Omega(r), \quad \text{mod } p \ \ (\S\,8),$$

we have

$$r^2B_1-r^4B_2+\ldots+(-1)^{\frac{1}{2}(p-1)}r^{p-3}B_{\frac{1}{2}(p-3)} \equiv -\frac{r+2}{2}-\Omega(r), \quad \text{mod } p. \qquad \text{(xviii.)}$$

51. Putting $r = 1$, since $\Omega(1) = 0$, this formula gives

$$B_1-B_2+B_3-\ldots+(-1)^{\frac{1}{2}(p-1)}B_{\frac{1}{2}(p-3)} \equiv -\tfrac{3}{2}, \quad \text{mod } p.^*$$

Putting $r = 2$, we find

$$\begin{aligned} 2^2B_1-2^4B_2+2^6B_3-\ldots&+(-1)^{\frac{1}{2}(p-1)}2^{p-3}B_{\frac{1}{2}(p-3)} \\ &\equiv -2-\Omega(2), \quad \text{mod } p, \\ &\equiv -2-\frac{1}{1}-\frac{1}{2}-\frac{1}{3}-\ldots-\frac{1}{k}, \quad \text{mod } p, \end{aligned}$$

where $$p = 2k+1.$$

Similarly, if $p = 3k+1$ or $3k+2$, we find, by putting $r = 3$,

$$\begin{aligned} 3^2B_1-3^4B_2+3^6B_3-\ldots&+(-1)^{\frac{1}{2}(p-1)}3^{p-3}B_{\frac{1}{2}(p-3)} \\ &\equiv -\frac{5}{2}-\frac{1}{1}-\frac{1}{2}-\frac{1}{3}-\ldots-\frac{1}{k}, \quad \text{mod } p, \end{aligned}$$

in both cases.

---

[*] This result may be derived immediately from the recurring formula

$$\frac{2n(2n-1)}{1.2}B_1-\frac{2n(2n-1)(2n-2)(2n-3)}{1.2.3.4}B_2+\ldots+(-1)^n\frac{2n(2n-1)}{1.2}B_{n-1} = n-1,$$

by putting $2n = p-1$.

52. It may be remarked that the formula (xviii.) of § 50 affords a simple proof of the result obtained in § 44. For the left-hand side of (xviii.) is unaltered, mod p, when $p-r$ is substituted for r; so that we have

$$\frac{r+2}{2}+\Omega(r)\equiv\frac{p-r+2}{2}+\Omega(p-r),\quad \text{mod } p,$$

and therefore $$\Omega(p-r)\equiv\Omega(r)+r.\quad \text{mod } p.$$

In the same manner, by substituting $p+r$ for r, we see that

$$\Omega(p+r)\equiv\Omega(r),\quad \text{mod } p,$$

and, in general, $$\Omega(np+r)\equiv\Omega(r),\quad \text{mod } p,$$

n being any positive integer.

The Function $A'_{2n}(x)$. (§§ 53–56.)

53. The function $A'_{2n}(x)$ is defined by the equation*

$$\begin{aligned}A'_{2n}(x)&=A_{2n}(x)-2^{2n}A_{2n}(\tfrac{1}{2}x)\\&=B_{2n}(x)-2^{2n}B_{2n}(\tfrac{1}{2}x)+(-1)^n(2^{2n}-1)\frac{B_n}{2n}.\end{aligned}$$

Putting $2n=p-1$, this equation becomes

$$A'_{p-1}(x)=B_{p-1}(x)-2^{p-1}B_{p-1}(\tfrac{1}{2}x)+(-1)^{\frac{1}{2}(p-1)}(2^{p-1}-1)\frac{B_{\frac{1}{2}(p-1)}}{p-1}.$$

Now $$pB_{\frac{1}{2}(p-1)}\equiv(-1)^{\frac{1}{2}(p-1)},\quad \text{mod } p,$$

and $$\frac{2^{p-1}-1}{p}\equiv 1+\frac{1}{3}+\frac{1}{5}+\ldots+\frac{1}{p-2},\quad \text{mod } p;\dagger$$

so that we obtain the formula

$$A'_{p-1}(x)\equiv B_{p-1}(x)-2^{p-1}B_{p-1}(\tfrac{1}{2}x)-\left(\frac{1}{1}+\frac{1}{3}+\ldots+\frac{1}{p-2}\right),\quad \text{mod } p,$$

and therefore, putting $$x=\frac{1}{r},$$

$$A'_{p-1}\left(\frac{1}{r}\right)\equiv\Omega(r)-\Omega(2r)-\left(\frac{1}{1}+\frac{1}{3}+\ldots+\frac{1}{p-2}\right),\quad \text{mod } p.\quad \text{(xix.)}$$

---

* *Quarterly Journal*, Vol. xxix., p. 93, or *Proc. Lond. Math. Soc.*, Vol. xxxi., p. 203.

† *Quarterly Journal*, Vol. xxxii., p. 21.

54. In general therefore, if p be any uneven Staudt factor for n,

$$2^{2n}A'_{2n}\left(\frac{1}{r}\right) \equiv \Omega(r)-\Omega(2r)-\left(\frac{1}{1}+\frac{1}{3}+\ldots+\frac{1}{p-2}\right), \text{ mod } p. \quad \text{(xx.)}$$

55. The values of $r^{2n}A'_{2n}\left(\frac{1}{r}\right)$ for $r = 2, 3, 4, 6$ are*

$$A'_{2n}(\tfrac{1}{2}) = 0, \qquad (1)$$

$$3^{2n}A'_{2n}(\tfrac{1}{3}) = (-1)^n(2^{2n}-1)(3^{2n}-3)\frac{B_n}{4n}, \qquad (2)$$

$$4^{2n}A'_{2n}(\tfrac{1}{4}) = (-1)^n 2Q_n, \qquad (3)$$

$$6^{2n}A'_{2n}(\tfrac{1}{6}) = (-1)^n 6T_n. \qquad (4)$$

56. Taking the last two equations and putting $2n = p-1$, we have

$$(-1)^{\frac{1}{2}(p-1)}2Q_{\frac{1}{2}(p-1)} \equiv \Omega(4)-\Omega(8)-\left(\frac{1}{1}+\frac{1}{3}+\ldots+\frac{1}{p-2}\right), \text{ mod } p,$$

$$(-1)^{\frac{1}{2}(p-1)}6T_{\frac{1}{2}(p-1)} = \Omega(6)-\Omega(12)-\left(\frac{1}{1}+\frac{1}{3}+\ldots+\frac{1}{p-2}\right), \text{ mod } p.$$

As an example, let $p = 11$. These general formulæ give

$$-2Q_5 \equiv \Omega(4)-\Omega(8)-(1+\tfrac{1}{3}+\ldots+\tfrac{1}{9}), \text{ mod } 11,$$

$$-6T_5 \equiv \Omega(6)-\Omega(1)-(1+\tfrac{1}{3}+\ldots+\tfrac{1}{9}), \text{ mod } 11.$$

Now, for all values of r, $\Omega(1) = 0$; if $r = 4$, $11 = 2r+r-1$, and therefore (§ 42) $\Omega(4) = 1+\frac{1}{2} \equiv 7$, mod 11; if $r = 6$, $11 = r+r-1$, and therefore (§ 42) $\Omega(6) = 1$; if $r = 8$, we have $m_1 = 3$, and

$$I(\tfrac{8}{3}) = 2, \quad I(\tfrac{16}{3}) = 5, \quad I(\tfrac{24}{3}) = 8;$$

so that $$\Omega(8) \equiv 8(\tfrac{1}{2}+\tfrac{1}{5}+\tfrac{1}{8}+\tfrac{1}{10}) \equiv 3, \text{ mod } 11.$$

Also $$1+\tfrac{1}{3}+\tfrac{1}{5}+\tfrac{1}{7}+\tfrac{1}{9} \equiv 5, \text{ mod } 11.$$

The formulæ therefore become

$$-2Q_5 \equiv 7-3-5, \text{ mod } 11,$$

$$-6T_5 \equiv 1-5, \text{ mod } 11,$$

giving $$Q_5 \equiv 6, \text{ mod } 11,$$

$$T_5 \equiv 8, \text{ mod } 11,$$

which are right, since $Q_5 = 2873041$, $T_5 = 67637281$.†

---

* *Quarterly Journal*, Vol. xxix., p. 107, or *Messenger*, Vol. xxvi., p. 178.

† *Quarterly Journal*, Vol. xxix., pp. 66, 76.

Residues of $B_{2n}\left(\frac{l}{r}\right)$ *and* $A'_{2n}\left(\frac{l}{r}\right)$, mod p. (§§ 57–60.)

57. We may obtain the residues of $B_{2n}\left(\frac{l}{r}\right)$ and $A'_{2n}\left(\frac{l}{r}\right)$ in exactly the same manner as the residues of $B_{2n}\left(\frac{1}{r}\right)$ and $A'_{2n}\left(\frac{1}{r}\right)$ were obtained in §§ 7 and 53.

From (iv.), § 4, we have

$$B_{p-1}(x) \equiv \frac{(p-1)!}{p} - \frac{x(x+1)\ldots(x+p-1)}{p}$$
$$\times\left\{\frac{1}{x}+\frac{1}{x+1}+\ldots+\frac{1}{x+p-1}\right\}, \text{ mod } p.$$

Let $x = \frac{l}{r}$ and suppose l prime to p; then, multiplying by r^{p-1},

$$r^{p-1}B_{p-1}\left(\frac{l}{r}\right) \equiv \frac{(p-1)!}{p}r^{p-1} - \frac{l(r+l)\ldots\{(p-1)r+l\}}{p}$$
$$\times\left\{\frac{1}{l}+\frac{1}{r+l}+\ldots+\frac{1}{(p-1)r+l}\right\}, \text{ mod } p.$$

Of the p numbers $l, r+l, \ldots, (p-1)r+l$ one is divisible by p, and we know that,* if $l = kp+t$ ($t > 0$ and $< p$),

$$\frac{l(r+l)\ldots\{(p-1)r+l\}}{p} \equiv (\mu_{p-t}+k+1)p.(p-1)!\,\{1+\Pi_t(r)\,p\}, \text{ mod } p,$$

where, if $t < p-1$,

$$\Pi_t(r) = \frac{\mu_1}{t+1}+\frac{\mu_2}{t+2}+\ldots+\frac{\mu_{p-t-1}}{p-1}+\frac{\mu_{p-t+1}+1}{1}+\frac{\mu_{p-t+2}+1}{2}+\ldots$$
$$\ldots+\frac{\mu_{p-1}+1}{t-1},$$

and $\Pi_{p-1}(r) = \frac{\mu_2+1}{1}+\frac{\mu_3+1}{2}+\ldots+\frac{\mu_{p-1}+1}{p-2}$.

Corresponding to $t = 0$, in which case $l = kp$, we have

$$\frac{l(r+l)\ldots\{(p-1)r+l\}}{p} \equiv k(p-1)!\,\{1+\Pi_0(r)\,p\}, \text{ mod } p,$$

where $$\Pi_0(r) = \frac{\mu_1}{1}+\frac{\mu_2}{2}+\ldots+\frac{\mu_{p-1}}{p-1}.$$

---

* *Messenger*, Vol. xxx., p. 82.

In these formulæ (as throughout this paper) μ_i is the least positive root of the congruence $p\mu_i + i \equiv 0$, mod r.

Consider now the series

$$\frac{1}{l} + \frac{1}{r+l} + \dots + \frac{1}{(p-1)\,r+l};$$

one of the denominators is the divisible number $(\mu_{p-t}+k+1)\,p$, and, since the others are $\equiv 1, 2, 3, \dots, p-1$, mod p, in some order, the sum of the other terms of the series $\equiv 0$, mod p.

Thus we have, if $t > 0$,

$$\begin{aligned} r^{p-1}B_{p-1}\left(\frac{l}{r}\right) &\equiv \frac{(p-1)!}{p}\,r^{p-1} - (\mu_{p-t}+k+1)\times(p-1)! \\ &\qquad\qquad \times\left\{1+\Pi_t(r)\right\}\frac{1}{(\mu_{p-t}+k+1)\,p} \\ &\equiv (p-1)!\left\{\frac{r^{p-1}-1}{p} - \Pi_t(r)\right\}, \text{ mod } p \\ &\equiv (p-1)!\left\{g_1(r) - \Pi_t(r)\right\}, \text{ mod } p \\ &\equiv \Pi_t(r) - g_1(r), \text{ mod } p, \end{aligned}$$

where
$$g_1(r) = \frac{\mu_1}{1} + \frac{\mu_2}{2} + \dots + \frac{\mu_{p-1}}{p-1}.$$

The quantity $g_1(r)$ is the same as $\Pi_0(r)$, and the result may therefore be written

$$r^{p-1}B_{p-1}\left(\frac{l}{r}\right) \equiv \Pi_t(r) - \Pi_0(r),^* \text{ mod } p. \qquad \text{(xx.)}$$

This formula is true also for $t = 0$, *i.e.*, for $l = kp$, the residue then being zero.

58. In general therefore, if p be any uneven Staudt factor for n, and if $l = kp+t$, then

$$r^{2n}B_{2n}\left(\frac{l}{r}\right) \equiv \Pi_t(r) - \Pi_0(r), \text{ mod } p. \qquad \text{(xxi.)}$$

---

* From this result we may derive the formula

$$r^2l^{p-3}B_1 - r^4l^{p-5}B_2 + \dots + (-1)^{\frac{1}{2}(p-1)}r^{p-3}l^2B_{\frac{1}{2}(p-3)} \equiv -\frac{r+2l}{2l} - \Pi_t(r) + \Pi_0(r), \text{ mod } p,$$

which includes (xviii.) of § 50.

59. Similarly, by proceeding as in § 53, we find that, p and l being as in the last section,

$$r^{2n}A'_{2n}\left(\frac{l}{r}\right) \equiv \Pi_t(r)-\Pi_t(2r)-\Pi_e(r)+\Pi_e(2r)$$
$$-\left(\frac{1}{1}+\frac{1}{3}+\frac{1}{5}+\ldots+\frac{1}{p-2}\right), \text{ mod } p.$$

60. The general expansions which have the quantities $a^{2n}B_{2n}\left(\frac{b}{a}\right)$ and $a^{2n}A'_{2n}\left(\frac{b}{a}\right)$ as coefficients are[*]

$$\frac{a}{2}\,\frac{\cos ax-\cos(2b-a)\,x}{\sin ax} = a^2B_2\left(\frac{b}{a}\right)2x-a^4B_4\left(\frac{b}{a}\right)\frac{(2x)^3}{3!}+\&c.,$$

$$\frac{a}{2}\,\frac{\sin(2b-a)}{\cos ax} = a^2A'_2\left(\frac{b}{a}\right)2x-a^4A'_4\left(\frac{b}{a}\right)\frac{(2x)^3}{3!}+\&c.$$

Putting $2b-a=c$, these formulæ become

$$\frac{a}{2}\,\frac{\cos ax-\cos cx}{\sin ax} = a^2B_2\left(\frac{a+c}{2a}\right)2x-a^4B_4\left(\frac{a+c}{2a}\right)\frac{(2x)^3}{3!}+\&c.,$$

$$\frac{a}{2}\,\frac{\sin cx}{\cos ax} = a^2A'_2\left(\frac{a+c}{2a}\right)2x-a^4A'_4\left(\frac{a+c}{2a}\right)\frac{(2x)^3}{3!}+\&c.$$

The formulæ of §§ 58 and 59 therefore enable us to assign the residues of the coefficients in these expansions.[†]

On the Residues of Bernoullian Functions for a Prime Modulus, including as special cases the Residues of the Bernoullian, Eulerian, and I-Numbers. By J. W. L. Glaisher. Read and received November 8th, 1900.

1. In previous papers[‡] the residues of $r^pB_p\left(\frac{1}{r}\right)$ and $r^{p-1}B_{p-1}\left(\frac{1}{r}\right)$, mod p, have been obtained and discussed. In the present paper these

---

[*] *Proc. Lond. Math. Soc.*, Vol. xxxi., pp. 206, 207.

[†] The corresponding expansions in which the suffixes of the B's and A''s are uneven were given in *Proc. Lond. Math. Soc.*, Vol. xxxii., p. 184.

[‡] *Proc. Lond. Math. Soc.*, Vol. xxxii., pp. 171–198, and Vol. xxxiii., pp. 27–56. The latter paper immediately precedes the present paper in this volume.

results are extended so as to give the residue of $r^{p-t}B_{p-t}\left(\frac{1}{r}\right)$, mod p, and, more generally, of $r^{n}B_{n}\left(\frac{1}{r}\right)$, mod p. This function includes the Bernoullian, Eulerian, and I-numbers, whose residues are thus assigned for any prime modulus.

Residue of $r^{p-2}B_{p-2}\left(\frac{1}{r}\right)$, mod p. (§§ 2–5.)

2. Starting with the formula (iv.) of § 4 of the preceding paper (p. 29), viz.,

$$B_{p-1}(x) \equiv \frac{(p-1)!}{p} - \frac{x(x+1)\dots(x+p-1)}{p}$$
$$\times \left\{\frac{1}{x} + \frac{1}{x+1} + \dots + \frac{1}{x+p-1}\right\}, \quad \text{mod } p, \quad \text{(i.)}$$

we find, since $\frac{d}{dx}B_{2n}(x) = (2n-1)B_{2n-1}(x)$,

$$(p-2)B_{p-2}(x) \equiv -\frac{x(x+1)\dots(x+p-1)}{p}\left\{\left(\frac{1}{x} + \frac{1}{x+1} + \dots + \frac{1}{x+p-1}\right)^2\right.$$
$$\left. - \frac{1}{x^2} - \frac{1}{(x+1)^2} - \dots - \frac{1}{(x+p-1)^2}\right\}, \quad \text{mod } p, \quad \text{(ii.)}$$

and therefore, putting $x = \frac{1}{r}$,

$$2r^{p-2}B_{p-2}\left(\frac{1}{r}\right) \equiv \frac{(r+1)(2r+1)\dots\{(p-1)r+1\}}{p}$$
$$\times \left[\left\{1 + \frac{1}{r+1} + \dots + \frac{1}{(p-1)r+1}\right\}^2 - 1 - \frac{1}{(r+1)^2} - \dots - \frac{1}{\{(p-1)r+1\}^2}\right],$$
$$\text{mod } p. \quad \text{(iii.)}$$

3. The $p-1$ numbers $r, 2r, 3r, \dots, (p-1)r$ when divided by p all leave different remainders, *i.e.*, the remainders must be 1, 2, 3, ..., $p-1$ in some order. Let $\mu_1, \mu_2, \mu_3, \dots, \mu_{p-1}$ be the respective quotients corresponding to these remainders. Then the $p-1$ numbers

$$\mu_1 p+1, \quad \mu_2 p+2, \quad \mu_3 p+3, \quad \dots, \quad \mu_{p-1}p+p-1$$

are (in some order) the same as the $p-1$ numbers

$$r, \quad 2r, \quad 3r, \quad \dots, \quad (p-1)r.$$

From the definition of the μ's it follows that μ_i is the least positive root of the congruence $p\mu_i + i \equiv 0$, mod r.[*] Adding 1 to each of the numbers $r, 2r, \dots, (p-1)r$, we obtain the numbers $r+1, 2r+1, \dots, (p-1)r+1$, which therefore are the same (in some order) as the numbers $\mu_1 p+2, \mu_2 p+3, \dots, \mu_{p-1}p+p$. Since the numbers $r, 2r, \dots, (p-1)r$ when divided by p leave remainders $1, 2, \dots, p-1$, it follows that the numbers $r+1, 2r+1, \dots, (p-1)r+1$ leave remainders $2, 3, \dots, p-1, 0$. Thus one of them is divisible by p, and this one, we see, is $(\mu_{p-1}+1)p$, which, putting $\mu_{p-1}+1 = m_1$, we write $m_1 p$.

4. Multiplying together the $p-1$ numbers $r+1, 2r+1, \dots, (p-1)r+1$, we have

$$\begin{aligned}(r+1)(2r+1)\dots\{(p-1)r+1\} &= m_1 p\,(\mu_1 p+2)(\mu_2 p+3)\dots(\mu_{p-2}p+p-1)\\ &\equiv m_1 p\times(p-1)!, \quad \text{mod } p^2,\end{aligned}$$

so that

$$\frac{(r+1)(2r+1)\dots\{(p-1)r+1\}}{p} \equiv -m_1, \quad \text{mod } p.$$

The formula (iii.) therefore gives

$$\begin{aligned}2r^{p-2}B_{p-2}\left(\frac{1}{r}\right) &\equiv -m_1\left\{\left(\frac{1}{m_1 p}+h_1\right)^2-\frac{1}{m_1^2p^2}-h_2\right\}\\ &\equiv -m_1\left(\frac{2h_1}{m_1 p}+h_1^2-h_2\right), \quad \text{mod } p,\end{aligned}$$

where

$$h_1 = 1+\frac{1}{\mu_1 p+2}+\frac{1}{\mu_2 p+3}+\dots+\frac{1}{\mu_{p-2}p+p-1},$$

$$h_2 = 1+\frac{1}{(\mu_1 p+2)^2}+\frac{1}{(\mu_2 p+3)^2}+\dots+\frac{1}{(\mu_{p-2}p+p-1)^2}.$$

5. Now

$$h_1 \equiv 1+\frac{1}{2}+\frac{1}{3}+\dots+\frac{1}{p-1}-\left\{\frac{\mu_1}{2^2}+\frac{\mu_2}{3^3}+\dots+\frac{\mu_{p-2}}{(p-1)^2}\right\}p, \text{ mod } p^2,$$

and therefore, since

$$1+\frac{1}{2}+\frac{1}{3}+\dots+\frac{1}{p-1} \equiv 0, \quad \text{mod } p^2 \ (p>3),$$

---

[*] The μ's are the same as in the preceding paper. The reasoning in the text is developed in greater detail in the *Messenger*, Vol. xxx., p. 77, *et seq.*, where the residue of the product $l(r+l)(2r+l)\dots\{(p-1)r+l\}$, mod p^3, is obtained.

we have $$h_1 \equiv -\left\{\frac{\mu_1}{2^2}+\frac{\mu_2}{3^2}+\ldots+\frac{\mu_{p-2}}{(p-1)^2}\right\}p, \quad \text{mod } p^2.$$

Also $$h_2 \equiv 1+\frac{1}{2^2}+\frac{1}{3^2}+\ldots+\frac{1}{(p-1)^2} \equiv 0, \quad \text{mod } p.$$

Therefore, if $p > 3$,

$$2r^{p-2}B_{p-2}\left(\frac{1}{r}\right) \equiv -\frac{2h_1}{p}, \quad \text{mod } p,$$

that is, $$r^{p-2}B_{p-2}\left(\frac{1}{r}\right) \equiv \frac{\mu_1}{2^2}+\frac{\mu_2}{3^2}+\ldots+\frac{\mu_{p-2}}{(p-1)^2}, \quad \text{mod } p. \quad \text{(iv.)}$$

Residue of $r^{p-3}B_{p-3}\left(\frac{1}{r}\right)$, mod p. (§ 6.)

6. Since $$\frac{d}{dx}B_{2n+1}(x) = 2nB_{2n}(x)+(-1)^{n-1}B_n,$$

we find by differentiating (ii.)

$$(p-2)(p-3)\,B_{p-3}(x)+(-1)^{\frac{1}{2}(p-1)}(p-2)\,B_{\frac{1}{2}(p-3)}$$
$$\equiv -\frac{x(x+1)\ldots(x+p-1)}{p}\left[\left(\frac{1}{x}+\frac{1}{x+1}+\ldots+\frac{1}{x+p-1}\right)^3\right.$$
$$-3\left(\frac{1}{x}+\frac{1}{x+1}+\ldots+\frac{1}{x+p-1}\right)\left\{\frac{1}{x^2}+\frac{1}{(x+1)^2}+\ldots+\frac{1}{(x+p-1)^2}\right\}$$
$$+2\left\{\frac{1}{x^3}+\frac{1}{(x+1)^3}+\ldots+\frac{1}{(x+p-1)^3}\right\}, \quad \text{mod } p. \qquad \text{(v.)}$$

Proceeding as before, *i.e.*, putting $x = \frac{1}{r}$, and expressing the system of numbers $r+1$, $2r+1$, ..., $(p-1)r+1$ in the μ-form, $\mu_1 p+2$, $\mu_2 p+3$, ..., $\mu_{p-2}p+p-1$, $m_1 p$, we find

$$6r^{p-3}B_{p-3}\left(\frac{1}{r}\right)+(-1)^{\frac{1}{2}(p-3}2r^{p-3}B_{\frac{1}{2}(p-3)}$$
$$\equiv m_1\left\{\left(\frac{1}{m_1 p}+h_1\right)^3-3\left(\frac{1}{m_1 p}+h_1\right)\left(\frac{1}{m_1^2p^2}+h_2\right)+2\left(\frac{1}{m_1^3p^3}+h_3\right)\right\}.$$
$$\text{mod } p, \quad \text{(vi.)}$$

where $$h_i = 1+\frac{1}{(\mu_1 p+2)^i}+\frac{1}{(\mu_2 p+3)^i}+\ldots+\frac{1}{(\mu_{p-2}p+p-1)^i}.$$

The right-hand side of (vi.)

$$= m_1\left\{\frac{3h_1^2-3h_2}{m_1 p}+h_1^3-3h_1h_2+2h_3\right\},$$

and, since h_1 and $h_3 \equiv 0$, mod p^2, and $h_2 \equiv 0$, mod p, (vi.) reduces to

$$6r^{p-3}B_{p-3}\left(\frac{1}{r}\right)+(-1)^{\frac{1}{2}(p-3)}2r^{p-3}B_{\frac{1}{2}(p-3)} \equiv -\frac{3h_2}{p}, \text{ mod } p. \quad \text{(vii.)}$$

Now
$$h_2 = 1+\frac{1}{(\mu_1 p+2)^2}+\frac{1}{(\mu_2 p+3)^2}+\dots+\frac{1}{(\mu_{p-2}p+p-1)^2}$$
$$\equiv 1+\frac{1}{2^2}+\frac{1}{3^2}+\dots+\frac{1}{(p-1)^2}$$
$$-2\left\{\frac{\mu_1}{2^3}+\frac{\mu_2}{3^3}+\dots+\frac{\mu_{p-2}}{(p-1)^3}\right\}p, \text{ mod } p^2,$$

and we know that*

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\dots+\frac{1}{(p-1)^2}=(-1)^{\frac{1}{2}(p-1)}\tfrac{2}{3}B_{\frac{1}{2}(p-3)}p, \text{ mod } p^2;$$

so that

$$-3h_2 \equiv (-1)^{\frac{1}{2}(p-3)}2B_{\frac{1}{2}(p-3)}p+6\left\{\frac{\mu_1}{2^3}+\frac{\mu_2}{3^3}+\dots+\frac{\mu_{p-2}}{(p-1)^3}\right\}p, \text{ mod } p^2.$$

The congruence (vii.) therefore reduces to

$$r^{p-3}B_{p-3}\left(\frac{1}{r}\right)+(-1)^{\frac{1}{2}(p-3)}\frac{r^{p-3}-1}{3}B_{\frac{1}{2}(p-3)} \equiv \frac{\mu_1}{2^3}+\frac{\mu_2}{3^3}+\dots+\frac{\mu_{p-2}}{(p-1)^3},$$
$$\text{mod } p. \quad \text{(viii.)}$$

Residue of $r^{p-t}B_{p-t}\left(\frac{1}{r}\right)$, mod p. (§§ 7–15.)

7. It will now be shown that in general, if $p>3$, and t be any even number less than p, and $p-t>1$,

$$r^{p-t}B_{p-t}\left(\frac{1}{r}\right) \equiv \frac{\mu_1}{2^t}+\frac{\mu_2}{3^t}+\dots+\frac{\mu_{p-2}}{(p-1)^t}, \text{ mod } p,$$

and, if t be any uneven number less than p,

$$r^{p-t}B_{p-t}\left(\frac{1}{r}\right)+(-1)^{\frac{1}{2}(p-t)}\frac{r^{p-t}-1}{t}B_{\frac{1}{2}(p-t)} \equiv \frac{\mu_1}{2^t}+\frac{\mu_2}{3^t}+\dots+\frac{\mu_{p-2}}{(p-1)^t},$$
$$\text{mod } p.$$

---

* *Quarterly Journal*, Vol. XXXI., p. 331, or Vol. XXXII., p. 11.

8. These results will be proved by the method employed in §§ 2–6 for obtaining the residues of $r^{p-2}B_{p-2}\left(\frac{1}{r}\right)$ and $r^{p-3}B_{p-3}\left(\frac{1}{r}\right)$, mod p.

The process therefore consists in differentiating $t-1$ times the formula (i.), or, which is the same thing, differentiating t times the formula

$$B_p(x)-x \equiv \frac{x(x+1)\dots(x+p-1)}{p}, \text{ mod } p,\text{*}$$

and making use of the relations

$$\frac{d}{dx}B_{2n}(x) = (2n-1)\,B_{2n-1}(x),$$

$$\frac{d}{dx}B_{2n+1}(x) = 2nB_{2n}(x)+(-1)^{n-1}B_n.$$

We thus obtain an expression for the residue of $B_{p-t}(x)$, mod p, in the form

$$\frac{x(x+1)\dots(x+p-1)}{p}X,$$

where X consists of terms which involve only the series

$$\frac{1}{x}+\frac{1}{x+1}+\dots+\frac{1}{x+p-1},$$

$$\frac{1}{x^2}+\frac{1}{(x+1)^2}+\dots+\frac{1}{(x+p-1)^2},$$

$$\dots \quad \dots \quad \dots \quad \dots \quad \dots$$

$$\frac{1}{x^t}+\frac{1}{(x+1)^t}+\dots+\frac{1}{(x+p-1)^t}.$$

We then replace x by $\frac{1}{r}$ and multiply by r^{p-t}, substitute $-m_1$ for the external factor $\frac{(r+1)(2r+1)\dots\{(p-1)\,r+1\}}{p}$, and replace each series

$$1+\frac{1}{(r+1)^i}+\dots+\frac{1}{\{(p-1)\,r+1\}^i}$$

by

$$\frac{1}{m_1^i p^i}+h_i$$

---

* The formula (i.) was deduced from this formula in the note to § 4 of the preceding paper (pp. 29, 30).

where $$h_t = 1 + \frac{1}{(\mu_1 p+2)^t} + \frac{1}{(\mu_2 p+3)^t} + \dots + \frac{1}{(\mu_{p-2} p+p-1)^t}.$$

Finally, by selecting that part of X which is not $\equiv 0$, mod p, we obtain the required residue.

9. Taking the steps of this process separately, we first consider the value of $\frac{d^t}{dx^t} B_p(x)$, which

$$= (p-1)(p-2)\dots(p-t)\,B_{p-t}(x),$$

if t is even,

and $$= (p-1)(p-2)\dots(p-t)B_{p-t}(x)$$
$$+ (-1)^{\frac{1}{2}(p-t-1)}(p-1)(p-2)\dots(p-t+1)\,B_{\frac{1}{2}(p-t)},$$

if t is uneven. Thus

$$\frac{d^t}{dx^t} B_p(x) \equiv t!\,B_{p-t}(x), \quad \text{mod } p,$$

if t is even, and

$$\equiv -t!\,B_{p-t}(x) - (-1)^{\frac{1}{2}(p-t)}(t-1)!\,B_{\frac{1}{2}(p-t)}, \quad \text{mod } p,$$

if t is uneven.

10. We next consider the quantity X.

We have

$$\frac{d^t}{dx^t}\, x(x+1)\dots(x+p-1) = x(x+1)\dots(x+p-1)\,X,$$

where, if we put

$$H_i = \frac{1}{(x+1)^i} + \frac{1}{(x+2)^i} + \dots + \frac{1}{(x+p-1)},$$

X is the sum of terms of the type

$$\left(\frac{1}{x}+H_1\right)^\alpha \left(\frac{1}{x^2}+H_2\right)^\beta \left(\frac{1}{x^3}+H_3\right)^\gamma \dots,$$

in which $$\alpha+2\beta+3\gamma+\dots = t.$$

Now, if we multiply out all these expressions, the terms in $\frac{1}{x^t}, \frac{1}{x^{t-1}}, \dots, \frac{1}{x^2}$ must disappear identically from X, for the derivatives of $x(x+1)\dots(x+p-1)$ are necessarily integral functions of x, and therefore no higher negative power of x than x^{-1} can occur in X.

The expanded terms in X must therefore be of the forms

$$\frac{aH_1^{\alpha-1}}{x} H_2^{\beta} H_3^{\gamma} \dots \quad \text{and} \quad H_1^{\alpha} H_2^{\beta} H_3^{\gamma} \dots .$$

11. When therefore we replace the series

$$1+\frac{1}{(r+1)^i}+\dots+\frac{1}{\{(p-1)\,r+1\}^i}$$

by

$$\frac{1}{m_1^i p^i}+h_i,$$

we have only to consider terms of the forms

$$\frac{ah_1^{\alpha-1}}{m_1 p} h_2^{\beta} h_3^{\gamma} \dots \quad \text{and} \quad h_1^{\alpha} h_2^{\beta} h_3^{\gamma} \dots$$

Terms of the second form are necessarily $\equiv 0$, mod p, since, if $p > 3$, $h_i \equiv 0$, mod p, for all values of i; and since, if $p > 3$, $h_1 \equiv 0$, mod p^2, the only term included in the first form which is not $\equiv 0$, mod p, is of the form

$$\frac{1}{m_1 p} h_{t-1}.$$

12. To determine the coefficient of this term we notice that it is the same as the coefficient of

$$\left(\frac{1}{x}+\frac{1}{x+1}+\dots\right)\left(\frac{1}{x^{t-1}}+\frac{1}{(x+1)^{t-1}}+\dots\right)$$

in $\frac{d^t}{dx^t} B_p(x)$. Denoting this coefficient by K_t, we see, by considering the terms in $\frac{d^{t-1}}{dx^{t-1}} B_p(x)$ which give rise to this term, that

$$K_t = -(t-2)\,K_{t-1}+(-1)^t\,(t-2)\,!,$$

whence

$$K_t = (-1)^t \frac{t!}{t-1}.$$

13. Replacing the external factor $\dfrac{(r+1)(2r+1)\dots\{(p-1)r+1\}}{p}$ by $-m_t$, we have therefore proved that

$$r^{p-t}\frac{d^t}{dx^t}B_p(x) \equiv (-1)^{t-1}\frac{t!}{t-1}\,\frac{h_{t-1}}{p}, \text{ mod } p. \qquad \text{(ix.)}$$

x being replaced by $\dfrac{1}{r}$ after the performance of the differentiations.

14. It is now necessary to separate the cases of t even and t uneven.

I. t even.

In this case, using the value of $\dfrac{d^t}{dx^t}B_p(x)$ obtained in § 9, the formula (ix.) gives

$$r^{p-t}t!\,B_{p-t}\left(\frac{1}{r}\right) \equiv -\frac{t!}{t-1}\,\frac{h_{t-1}}{p}, \text{ mod } p,$$

where

$$h_{t-1} = 1+\frac{1}{(\mu_1 p+2)^{t-1}}+\frac{1}{(\mu_2 p+3)^{t-1}}+\dots+\frac{1}{(\mu_{p-2}p+p-1)^{t-1}}$$

$$\equiv 1+\frac{1}{2^{t-1}}+\frac{1}{3^{t-1}}+\dots+\frac{1}{(p-1)^{t-1}}$$

$$-(t-1)\left\{\frac{\mu_1}{2^t}+\frac{\mu_2}{3^t}+\dots+\frac{\mu_{p-2}}{(p-1)^t}\right\}p, \text{ mod } p^2.$$

Since t is even, and $p>3$,

$$1+\frac{1}{2^{t-1}}+\frac{1}{3^{t-1}}+\dots+\frac{1}{(p-1)^{t-1}} \equiv 0, \text{ mod } p^2;$$

and therefore

$$h_{t-1} \equiv -(t-1)\left\{\frac{\mu_1}{2^t}+\frac{\mu_2}{3^t}+\dots+\frac{\mu_{p-2}}{(p-1)^t}\right\}p, \text{ mod } p^2.$$

In this case therefore the formula becomes

$$r^{p-t}B_{p-t}\left(\frac{1}{r}\right) \equiv \frac{\mu_1}{2^t}+\frac{\mu_2}{3^t}+\dots+\frac{\mu_{p-2}}{(p-1)^t}, \text{ mod } p. \qquad \text{(x.)}$$

II. t uneven.

In this case we have, from § 9 and formula (ix.),

$$-r^{p-t}t!\,B_{p-t}\left(\frac{1}{r}\right)-(-1)^{\frac{1}{2}(p-t)}\,r^{p-t}(t-1)!\,B_{\frac{1}{2}(p-t)} \equiv \frac{t!}{t-1}\,\frac{h_{t-1}}{p}, \text{ mod } p,$$

As before,

$$h_{t-1} \equiv 1 + \frac{1}{2^{t-1}} + \frac{1}{3^{t-1}} + \dots + \frac{1}{(p-1)^{t-1}}$$

$$-(t-1)\left\{\frac{\mu_1}{2^t} + \frac{\mu_2}{3^t} + \dots + \frac{\mu_{p-2}}{(p-1)^t}\right\}p, \quad \text{mod } p^2.$$

Since t is uneven,

$$1 + \frac{1}{2^{t-1}} + \frac{1}{3^{t-1}} + \dots + \frac{1}{(p-1)^{t-1}} \equiv (-1)^{\frac{1}{2}(p-t)-1}\frac{(t-1)\,B_{\frac{1}{2}(p-t)}}{t}p, \quad \text{mod } p^2;^{[*]}$$

and therefore

$$h_{t-1} \equiv (-1)^{\frac{1}{2}(p-t)-1}\frac{(t-1)\,B_{\frac{1}{2}(p-t)}}{t}p - (t-1)\left\{\frac{\mu_1}{2^t} + \frac{\mu_2}{3^t} + \dots + \frac{\mu_{p-2}}{(p-1)^t}\right\}p,$$

$$\text{mod } p^2.$$

Thus we have

$$-r^{p-t}\,t!\,B_{p-t}\left(\frac{1}{r}\right) - (-1)^{\frac{1}{2}(p-t)}r^{p-t}(t-1)!\,B_{\frac{1}{2}(p-t)}$$

$$\equiv (-1)^{\frac{1}{2}(p-t)-1}(t-1)!\,B_{\frac{1}{2}(p-t)} - t!\left\{\frac{\mu_1}{2^t} + \frac{\mu_2}{3^t} + \dots + \frac{\mu_{p-2}}{(p-1)^t}\right\}, \text{mod } p,$$

that is, dividing by $t!$,

$$r^{p-t}B_{p-t}\left(\frac{1}{r}\right) + (-1)^{\frac{1}{2}(p-t)}\frac{r^{p-t}-1}{t}B_{\frac{1}{2}(p-t)} \equiv \frac{\mu_1}{2^t} + \frac{\mu_2}{3^t} + \dots + \frac{\mu_{p-2}}{(p-1)^t},$$

$$\text{mod } p. \quad \text{(xi.)}$$

The formulæ (x.) and (xi.) are those enunciated in § 7.[†]

15. If q is any number prime to p,

$$\frac{1}{q^t} \equiv q^{p-t-1}, \quad \text{mod } p;$$

---

[*] *Quarterly Journal*, Vol. xxxi., p. 331.

[†] If in §§ 8–14 we put $x = \frac{l}{r}$, and substitute for $r+l$, $2r+l$, ..., $(p-1)r+l$ the system $\mu_1 p + l + 1$, $\mu_2 p + l + 2$, ..., $\mu_{p-l-1}p + p - 1$, $(\mu_{p-l}+1)p$, $(\mu_{p-l+1}+1)p+1$, $(\mu_{p-l+2}+1)p+2$, ..., $(\mu_{p-1}+1)p+l-1$ as in the *Messenger*, Vol. xxx., p. 79, we may obtain formulæ, corresponding to (x.) and (xi.), for the residue of $r^{p-t}B_{p-t}\left(\frac{l}{r}\right)$. The residues in the case of some particular values of l are noticed in §§ 45–50.

and therefore the formula (x.) may be written

$$r^{p-t}B_{p-t}\left(\frac{1}{r}\right) \equiv \mu_1 2^{p-t-1}+\mu_2 3^{p-t-1}+\ldots+\mu_{p-2}(p-1)^{p-t-1}, \text{ mod } p.$$

Putting $p-t = s$, we have therefore, if s is any uneven number > 1, and $p > s$,

$$r^sB_s\left(\frac{1}{r}\right) \equiv \mu_1 2^{s-1}+\mu_2 3^{s-1}+\ldots+\mu_{p-2}(p-1)^{s-1}, \text{ mod } p. \quad \text{(xii.)}$$

Similarly, we deduce from (xi.) that, if s is any even number and $p>s$,

$$r^sB_s\left(\frac{1}{r}\right)+(-1)^{\frac{1}{2}s-1}\frac{r^s-1}{s}B_{\frac{1}{2}s} \equiv \mu_1 2^{s-1}+\mu_2 3^{s-1}+\ldots+\mu_{p-2}(p-1)^{s-1},$$
$$\text{mod } p. \quad \text{(xiii.)}$$

Residues of $r^{2n+1}B_{2n+1}\left(\frac{1}{r}\right)$ *and* $r^{2n}B_{2n}\left(\frac{1}{r}\right)$, mod p. (§§ 16-20.)

16. In general, for all values of $p>3$, we have

$$r^{2n+1}B_{2n+1}\left(\frac{1}{r}\right) \equiv \mu_1 2^{2n}+\mu_2 3^{2n}+\ldots+\mu_{p-2}(p-1)^{2n}, \text{ mod } p. \quad \text{(xiv.)}$$

This formula was shown in (xii.) to be true when $p>2n+1$. It will now be shown to be true also when $p<2n+1$,* if $p-1$ is not a divisor of $2n$.

Let $2n+1 = k(p-1)+s$, so that s is uneven and $<p-1$. Then

$$r^{2n+1}B_{2n+1}\left(\frac{1}{r}\right) \equiv r^{k(p-1)+s}B_{k(p-1)+s}\left(\frac{1}{r}\right), \text{ mod } p,$$
$$\equiv r^sB_s\left(\frac{1}{r}\right), \text{ mod } p,†$$

and therefore, by (xii.), if $s>1$, *i.e.*, if $p-1$ is not a divisor of $2n$,

$$r^{2n+1}B_{2n+1}\left(\frac{1}{r}\right) \equiv \mu_1 2^{s-1}+\mu_2 3^{s-1}+\ldots+\mu_{p-2}(p-1)^{s-1}, \text{ mod } p,$$
$$\equiv \mu_1 2^{2n-k(p-1)}+\mu_2 3^{2n-k(p-1)}+\ldots+\mu_{p-2}(p-1)^{2n-k(p-1)},$$
$$\text{mod } p,$$
$$\equiv \mu_1 2^{2n}+\mu_2 3^{2n}+\ldots+\mu_{p-2}(p-1)^{2n}, \text{ mod } p.$$

---

* When $2n+1 = p$ the formula is $r^pB_p\left(\frac{1}{r}\right) \equiv -\mu_{p-1}$, mod p (*Proc. Lond. Math. Soc.*, Vol. XXXII., p. 174).

† For $B_n(x) \equiv B_{n-k(p-1)}(x)$, mod p, if p is not a factor of the denominator of x (*Proc. Lond. Math. Soc.*, Vol. XXXI., p. 206).

17. In the same manner we can show that, for all values of p, such that $p-1$ is not a divisor of $2n$,

$$r^{2n}B_{2n}\left(\frac{1}{r}\right)+(-1)^{n-1}(r^{2n}-1)\frac{B_n}{2n}$$
$$\equiv \mu_1 2^{2n-1}+\mu_2 3^{2n-1}+\ldots+\mu_{p-2}(p-1)^{2n-1},\ \text{mod}\ p. \quad \text{(xv.)}$$

For, putting $2n = k(p-1)+s$, so that s is even and >0 and $<p-1$, we have

$$r^{2n}B_{2n}\left(\frac{1}{r}\right) \equiv r^s B_s\left(\frac{1}{r}\right),\ \text{mod}\ p,$$

$$r^{2n}-1 \equiv r^s-1,\ \text{mod}\ p,$$

$$(-1)^n\frac{B_n}{2n} \equiv (-1)^{\frac{1}{2}s}\frac{B_{\frac{1}{2}s}}{s},\ \text{mod}\ p,\text{*}$$

and
$$q^{2n} \equiv q^s,\ \text{mod}\ p,$$

q being any number prime to p.

The formula (xv.) therefore reduces to

$$r^s B_s\left(\frac{1}{r}\right)+(-1)^{\frac{1}{2}s-1}(r^s-1)\frac{B_{\frac{1}{2}s}}{s} \equiv \mu_1 2^{s-1}+\mu_2 3^{\ -1}+\ldots+\mu_{p-2}(p-1)^{s-1},$$
$$\text{mod}\ p,$$

which is (xiii.).

18. The formula (xiv.), viz.,

$$r^{2n+1}B_{2n+1}\left(\frac{1}{r}\right) \equiv \mu_1 2^{2n}+\mu_2 3^{2n}+\ldots+\mu_{p-2}(p-1)^{2n},\ \text{mod}\ p,$$

may be transformed into other more convenient forms as follows.

We have, if $2n$ is not a multiple of $p-1$,

$$0 = \mu_1 1^{2n}+\mu_2 2^{2n}+\ldots+\mu_{p-1}(p-1)^{2n},\quad \text{mod}\ p,\text{†}$$

---

* *Messenger*, Vol. XXIX., pp. 60, 129.

† To prove this formula, we notice that $\mu_i+\mu_{p-i}=r-1$, and

$$1^{2n} \equiv (p-1)^{2n},\ \text{mod}\ p,\quad 2^{2n} \equiv (p-2)^{2n},\ \text{mod}\ p,\ \ldots;$$

so that

$$\mu_1 1^{2n}+\mu_2 2^{2n}+\ldots+\mu_{p-1}(p-1)^{2n} \equiv (r-1)\left\{1^{2n}+2^{2n}+\ldots+\left(\frac{p-1}{2}\right)^{2n}\right\},\ \text{mod}\ p,$$
$$\equiv \frac{r-1}{2}\left\{1^{2n}+2^{2n}+\ldots+(p-1)^{2n}\right\},\ \text{mod}\ p,$$
$$\equiv \frac{r-1}{2}B_{2n+1}(p),\ \text{mod}\ p.$$

Now every term in the expression for $B_{2n+1}(p)$ in ascending powers of p has p^2 or and, subtracting this formula from (xiv.), we find

$$r^{2n+1}B_{2n+1}\left(\frac{1}{r}\right) \equiv -\mu_1 1^{2n}+(\mu_1-\mu_2)\,2^{2n}+(\mu_2-\mu_3)\,3^{2n}+\dots$$
$$+(u_{p-2}-\mu_{p-1})(p-1)^{2n}, \quad \text{mod } p.$$

This expression corresponds exactly to the definition of $\Omega(r)$ in § 9 (p. 32) of the preceding paper, viz.,

$$\Omega(r) = -\frac{\mu_1}{1}+\frac{\mu_1-\mu_2}{2}+\frac{\mu_2-\mu_3}{3}+\dots+\frac{\mu_{p-2}-\mu_{p-1}}{p-1},$$

and, just as $\Omega(r)$ was transformed into various other expressions by the use of the formula

$$1+\frac{1}{2}+\frac{1}{3}+\dots+\frac{1}{p-1} \equiv 0, \quad \text{mod } p,$$

so we may transform the expression for the residue of $r^{2n+1}B_{2n+1}\left(\frac{1}{r}\right)$ into corresponding expressions by means of the formula

$$1^{2n}+2^{2n}+3^{2n}+\dots+(p-1)^{2n} \equiv 0, \quad \text{mod } p,\text{*}$$

in which $2n$ must not be a multiple of $p-1$.

19. The most important formulæ so obtained correspond to (ix.) of § 16, and (xi.) of § 24 in the preceding paper, and are as follows

$$r^{2n+1}B_{2n+1}\left(\frac{1}{r}\right) \equiv r\,(\beta_1^{2n}+\beta_2^{2n}+\beta_3^{2n}+\dots), \quad \text{mod } p, \quad \text{(xvi.)}$$

where
$$p\mu_1 \equiv -1, \quad \text{mod } r,$$

$$\beta_i = K\left(\frac{ir}{\mu_1}\right);$$

and
$$r^{2n+1}B_{2n+1}\left(\frac{1}{r}\right) \equiv -r\,(a_1^{2n}+a_2^{2n}+a_3^{2n}+\dots), \quad \text{mod } p, \quad \text{(xvii.)}$$

---

some higher power of p in the numerator, except the last term $(-1)^{n-1}B_n p$, and this term cannot have p in its denominator unless n is a multiple of $\frac{p-1}{2}$. Thus $B_{2n+1}(p) \equiv 0$, mod p, unless $2n$ is a multiple of $p-1$, which proves the formula in the text.

* For $1^{2n}+2^{2n}+\dots+(p-1)^{2n} = B_{2n+1}(p)$, which has just been shown (in the preceding note) to be $\equiv 0$, mod p, when $2n$ is not a multiple of $p-1$.

where
$$pm_1 \equiv 1, \text{ mod } r,$$
$$a_i = I\left(\frac{ir}{\mu_1}\right).^*$$

The functions $K\left(\frac{b}{a}\right)$ and $I\left(\frac{b}{a}\right)$ denote respectively the integers next above, and next below, $\frac{b}{a}$ when $\frac{b}{a}$ is fractional; but when $\frac{b}{a}$ is integral
$$K\left(\frac{b}{a}\right) = I\left(\frac{b}{a}\right) = \frac{b}{a}.$$

The quantities μ_1 and m_1 are connected by the relation $\mu_1+m_1 = r$, and we use μ_1 or m_1, *i.e.*, the formula (xvi.) or (xvii.), according as $\mu_1 <$ or $> \frac{1}{2}r$ (§ 27 of the preceding paper).

20. We may notice the particular cases (corresponding to § 42 of the preceding paper†) in which $p = kr+1$ or $kr+r-1$, viz.,

I. If $p = kr+1$,
$$r^{2n+1}B_{2n+1}\left(\frac{1}{r}\right) \equiv -r^{2n+1}(1^{2n}+2^{2n}+\ldots+k^{2n}), \text{ mod } p.$$

II. If $p = kr+r-1$,
$$r^{2n+1}B_{2n+1}\left(\frac{1}{r}\right) \equiv r^{2n+1}(1^{2n}+2^{2n}+\ldots+k^{2n}), \text{ mod } p.$$

---

[*] In the transition from the μ-form of $\Omega(r)$ to the m-form in § 19 of the preceding paper, each denominator $p-i$ is replaced by $-i$; in the corresponding transition for $r^{2n+1}B_{2n+1}\left(\frac{1}{r}\right)$, $(p-i)^{2n}$ is replaced by i^{2n}; so that the m-form for the residue of $r^{2n+1}B_{2n+1}\left(\frac{1}{r}\right)$ has the opposite sign to that of the m-form of $\Omega(r)$, and therefore also the expressions derived from the m-form of $r^{2n+1}B_{2n+1}\left(\frac{1}{r}\right)$ have the opposite sign to the corresponding $\Omega(r)$ expressions.

[†] All the investigations relating to $\Omega(r)$ contained in §§ 10-44 of the preceding paper (pp. 32-47) hold good also with respect to the residue of $r^{2n+1}B_{2n+1}\left(\frac{1}{r}\right)$, when $2n$ is not a multiple of $p-1$, the exponent $2n$ replacing the exponent -1; but, as pointed out in the preceding note, the sign is different in the case of the m-form and the expressions derived from it.

Residue of E_n, mod p. (§§ 21–25.)

21. Since $$4^{2n+1}B_{2n+1}(\tfrac{1}{4}) = (-1)^{n+1}E_n,$$
where E_n is the nth Eulerian number, the formula (xiv.) gives, by putting $r = 4$,

$$(-1)^{n+1}E_n \equiv \mu_1 2^{2n} + \mu_2 3^{2n} + \ldots + \mu_{p-2}(p-1)^{2n}, \quad \text{mod } p,$$

where μ_i is the least positive root of

$$p\mu_i + 1 \equiv 0, \quad \text{mod } 4.$$

When $p = 4k+1$, $\mu_1 = 3$, $\mu_2 = 2$, $\mu_3 = 1$, $\mu_4 = 0$, and this formula becomes

$$(-1)^{n+1}E_n \equiv 3.2^{2n} + 2.3^{2n} + 1.4^{2n} + 0.5^{2n} + \ldots + 1\,(p-1)^{2n}, \quad \text{mod } p,$$

and we know* that, if $p = 4k+1$, and $2n$ is not a multiple of $p-1$,

$$1^{2n} + 5^{2n} + \;9^{2n} + \ldots + (p-4)^{2n} \equiv S, \quad \text{mod } p,$$
$$2^{2n} + 6^{2n} + 10^{2n} + \ldots + (p-3)^{2n} \equiv -S, \quad \text{mod } p,$$
$$3^{2n} + 7^{2n} + 11^{2n} + \ldots + (p-2)^{2n} \equiv -S, \quad \text{mod } p,$$

where $$S = 4^{2n} + 8^{2n} + 12^{2n} + \ldots + (p-1)^{2n}.$$

Thus we find

$$(-1)^{n+1}E_n \equiv -4\,\{4^{2n} + 8^{2n} + \ldots + (p-1)^{2n}\}, \quad \text{mod } p,$$
$$\equiv -4^{2n+1}(1^{2n} + 2^{2n} + \ldots + k^{2n}), \quad \text{mod } p,$$

where $$k = \tfrac{1}{4}(p-1);$$

and therefore $$E_n \equiv (-1)^n 4^{2n+1}(1^{2n} + 2^{2n} + \ldots + k^{2n}), \quad \text{mod } p.$$

22. When $p = 4k+3$, we have $\mu_1 = 1$, $\mu_2 = 2$, $\mu_3 = 3$, $\mu_4 = 0$, and the formula becomes

$$(-1)^{n+1}E_n \equiv 1.2^{2n} + 2.3^{2n} + 3.4^{2n} + 0.5^{2n} + \ldots + 1\,(p-1)^{2n}, \quad \text{mod } p,$$

and, in this case,†

$$1^{2n} + 5^{2n} + \;9^{2n} + \ldots + (p-2)^{2n} \equiv -S, \quad \text{mod } p,$$
$$2^{2n} + 6^{2n} + 10^{2n} + \ldots + (p-1)^{2n} \equiv -S, \quad \text{mod } p,$$
$$3^{2n} + 7^{2n} + 11^{2n} + \ldots + (p-4)^{2n} \equiv S, \quad \text{mod } p,$$

where $$S = 4^{2n} + 8^{2n} + 12^{2n} + \ldots + (p-3)^{2n}.$$

---

* *Messenger*, Vol. xxx., p. 156.

† *Messenger, loc. cit.*

Thus we find

$$(-1)^{n+1}E_n \equiv 4\,\{4^{2n}+8^{2n}+\ldots+(p-3)^{2n}\},\ \bmod p,$$
$$\equiv 4^{2n+1}(1^{2n}+2^{2n}+\ldots+k^{2n}),\ \bmod p,$$

where $k=\tfrac{1}{4}(p-3)$;

and therefore $E_n \equiv (-1)^{n+1}4^{2n+1}(1^{2n}+2^{2n}+\ldots+k^{2n}),\ \bmod p.$

23. In general, therefore,

$$(-1)^n E_n \equiv \pm 4^{2n+1}(1^{2n}+2^{2n}+\ldots+k^{2n}),\ \bmod p, \qquad \text{(xviii.)}$$

where k is the greatest integer contained in $\frac{p}{4}$, and the upper or lower sign is to be taken according as p is of the form $4k+1$ or $4k+3$.*

24. The most interesting particular cases of (xviii.) are when $n=\tfrac{1}{2}(p-3)$, $n=\tfrac{1}{2}(p-5)$, ...

Putting $n=\tfrac{1}{2}(p-3)$, and supposing $p=4k+1$, (xviii.) gives

$$E_{\frac{1}{2}(p-3)} \equiv -4^{p-2}(1^{p-3}+2^{p-3}+\ldots+k^{p-3}),\ \bmod p,$$
$$\equiv -\tfrac{1}{4}\left(1+\frac{1}{2^2}+\ldots+\frac{1}{k^2}\right),\ \bmod p.$$

We obtain the same formula if $p=4k+3$; so that we have, for all values of p,

$$E_{\frac{1}{2}(p-3)} \equiv -\tfrac{1}{4}\left(1+\frac{1}{2^2}+\ldots+\frac{1}{k^2}\right),\ \bmod p, \qquad \text{(xix.)}$$

where k is the greatest integer contained in $\frac{p}{4}$.

Similarly, by putting $n=\tfrac{1}{2}(p-5)$, $\tfrac{1}{2}(p-7)$, ..., we find from (xviii.)

$$E_{\frac{1}{2}(p-5)} \equiv -\frac{1}{4^3}\left(1+\frac{1}{2^4}+\ldots+\frac{1}{k^4}\right),\ \bmod p,$$

$$E_{\frac{1}{2}(p-7)} \equiv -\frac{1}{4^5}\left(1+\frac{1}{2^6}+\ldots+\frac{1}{k^6}\right),\ \bmod p,$$

... ...

k being as before.†

---

* These formulæ might have been deduced directly from § 20.

† These formulæ might have been deduced directly from (x.) of § 14.

The corresponding formula for $n = \frac{1}{2}(p-1)$ is

$$E_{\frac{1}{2}(p-1)} \equiv 0 \text{ or } -2, \mod p,$$

according as p is of the form $4k+1$ or $4k+3$.*

25. We may state these results also as follows:

$$\begin{aligned} E_n &\equiv 0 \text{ or } (-1)^n\, 2, \mod 2n+1, \text{ if } 2n+1 \text{ is prime,} \\ &\equiv -\frac{1}{4}\left(1+\frac{1}{2^2}+\ldots+\frac{1}{k^2}\right), \mod 2n+3, \text{ if } 2n+3 \text{ is prime,} \\ &\equiv -\frac{1}{4^3}\left(1+\frac{1}{2^4}+\ldots+\frac{1}{k^4}\right), \mod 2n+5, \text{ if } 2n+5 \text{ is prime,} \\ &\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \end{aligned}$$

where k is the greatest integer contained in $\frac{k}{4}$.

More generally, if p is an uneven Staudt factor for n (*i.e.*, if $p-1$ is a divisor of $2n$),

$$E_n \equiv 0 \text{ or } (-1)^n\, 2, \mod p;$$

if p is an uneven Staudt factor for $n+1$,

$$E_n \equiv -\frac{1}{4}\left(1+\frac{1}{2^2}+\ldots+\frac{1}{k^2}\right), \mod p;$$

if p is an uneven Staudt factor for $n+2$,

$$E_n \equiv -\frac{1}{4^3}\left(1+\frac{1}{2^4}+\ldots+\frac{1}{k^4}\right), \mod p,$$

and so on.

Residues of I_n, mod p. (§§ 26–29.)

26. Since $$3^{2n+1}B_{2n+1}\left(\tfrac{1}{3}\right) \equiv (-1)^{n+1} I_n, \mod p,$$

the formula (xvi.) gives, by putting $r = 3$,

$$(-1)^{n+1} I_n \equiv \mu_1 2^{2n} + \mu_2 3^{2n} + \ldots + \mu_{p-2}(p-1)^{2n}, \mod p,$$

where μ_i is the least positive root of

$$p\mu_i + 1 \equiv 0, \mod 3.$$

---

* *Proc. Lond. Math. Soc.*, Vol. xxxii., p. 176.

When $p = 3k+1$, $\mu_1 = 2$, $\mu_2 = 1$, $\mu_3 = 0$, and the formula becomes

$$(-1)^{n+1} I_n \equiv 2.2^{2n}+1.3^{2n}+0.4^{2n}+2.5^{2n}+\ldots+1\,(p-1)^{2n}, \text{ mod } p.$$

Now, if $p = 3k+1$, and $p-1$ is not a multiple of $2n$,

$$1^{2n}+4^{2n}+7^{2n}+\ldots+(p-3)^{2n} \equiv S, \quad \text{mod } p,$$

$$2^{2n}+5^{2n}+8^{2n}+\ldots+(p-2)^{2n} \equiv -2S, \quad \text{mod } p,$$

where $\qquad S = 3^{2n}+6^{2n}+9^{2n}+\ldots+(p-1)^{2n}$.*

Thus we find

$$\begin{aligned}(-1)^{n+1} I_n &\equiv -3\left\{3^{2n}+6^{2n}+\ldots+(p-1)^{2n}\right\}, \text{ mod } p,\\ &\equiv -3^{2n+1}(1^{2n}+2^{2n}+\ldots+k^{2n}), \text{ mod } p,\end{aligned}$$

where $\qquad k = \tfrac{1}{3}(p-1)$;

and therefore $\qquad I_n \equiv (-1)^n\, 3^{2n+1}(1^{2n}+2^{2n}+\ldots+k^{2n})$, mod p.

27. By an exactly similar procedure we can show that, when $p = 3k+2$,

$$I_n \equiv (-1)^{n+1}\, 3^{2n+1}(1^{2n}+2^{2n}+\ldots+k^{2n}), \text{ mod } p.$$

Thus, generally, for all values of n,

$$(-1)^n I_n \equiv \pm 3^{2n+1}(1^{2n}+2^{2n}+\ldots+k^{2n}), \text{ mod } p, \qquad \text{(xx.)}$$

where k is the greatest integer contained in $\frac{p}{3}$, and the upper or lower sign is to be taken according as p is of the form $3k+1$ or $3k+2$.

28. As particular cases we derive, as in § 24, the formulæ

$$\left.\begin{aligned}(-1)^{\frac12(p-3)} I_{\frac12(p-3)} &\equiv \pm\frac{1}{3}\left(1+\frac{1}{2^2}+\ldots+\frac{1}{k^2}\right), \text{ mod } p\\ (-1)^{\frac12(p-5)} I_{\frac12(p-5)} &\equiv \pm\frac{1}{3^3}\left(1+\frac{1}{2^4}+\ldots+\frac{1}{k^4}\right), \text{ mod } p\\ (-1)^{\frac12(p-7)} I_{\frac12(p-7)} &\equiv \pm\frac{1}{3^5}\left(1+\frac{1}{2^6}+\ldots+\frac{1}{k^6}\right), \text{ mod } p\\ \ldots \quad \ldots \quad \ldots \quad &\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots\end{aligned}\right\}, \qquad \text{(xxi.)}$$

where k is the greatest integer contained in $\frac{p}{3}$, and the upper or lower sign is to be taken according as p is of the form $3k+1$ or $3k+2$.*

---

* *Messenger*, Vol. xxx., p. 157.

The corresponding formula for the case $n = \frac{1}{2}(p-1)$ is

$$(-1)^{\frac{1}{2}(p-1)} I_{\frac{1}{2}(p-1)} \equiv 0 \text{ or } 1, \bmod p,$$

according as p is of the form $3k+1$ or $3k+2$.†

29. Thus, generally, if p is an uneven Staudt factor for n,

$$(-1)^n I_n \equiv 0 \text{ or } 1, \bmod p;$$

if p is an uneven Staudt factor for $n+1$,

$$(-1)^n I_n \equiv \pm \frac{1}{3}\left(1+\frac{1}{2^2}+\ldots+\frac{1}{k^2}\right), \bmod p;$$

if p is an uneven Staudt factor for $n+2$,

$$(-1)^n I_n \equiv \pm \frac{1}{3^3}\left(1+\frac{1}{2^4}+\ldots+\frac{1}{k^4}\right), \bmod p;$$

and so on. As before, k is the greatest integer contained in $\frac{p}{3}$, and the upper or lower sign is to be taken according as p is of the form $3k+1$ or $3k+2$.

I have verified these formulæ in a number of cases by means of the table of I_n up to $n = 13$ given in *Proc. Lond. Math. Soc.*, Vol. XXXI., p. 224. The corresponding Staudt factors were given in Vol. XXXII., p. 177.

Residue of $\frac{B_n}{n}$. (§§ 30–32.)

30. Putting $r = 2$ in formula (xv.), § 17, we have

$$2^{2n}B_{2n}(\tfrac{1}{2})+(-1)^{n-1}(2^{2n}-1)\frac{B_n}{2n} \equiv \mu_1 2^{2n-1}+\mu_2 3^{2n-1}+\ldots+\mu_{p-2}(p-1)^{2n-1}, \bmod p,$$

where μ_i is given by $p\mu_i + i \equiv 0, \bmod p$. Thus $\mu_1 = 1$, $\mu_2 = 0$. Also

$$2^{2n}B_{2n}(\tfrac{1}{2}) = (-1)^n (2^{2n}-1)\frac{B_n}{n};$$

---

* Formula (xx.) could be derived directly from § 20, and formula (xxi.) and the following formulæ from (x.) of § 14. Similar formulæ containing fewer terms are given in § 43.

† *Proc. Lond. Math. Soc.*, Vol. XXXII., p. 177.

and therefore the formula becomes

$$(-1)^n(2^{2n}-1)\frac{B_n}{2n} \equiv 2^{2n-1}+4^{2n-1}+\ldots+(p-1)^{2n-1}, \quad \text{mod } p,$$

$$\equiv 2^{2n-1}(1+2^{2n-1}+\ldots+k^{2n-1}), \quad \text{mod } p, \text{(xxii.)}$$

where $k = \frac{1}{2}(p-1)$.

31. Putting $n = \frac{1}{2}(p-3)$, (xxii.) gives

$$(-1)^{\frac{1}{2}(p-3)}(2^{p-3}-1)\frac{B_{\frac{1}{2}(p-3)}}{p-3} \equiv 2^{p-4}(1^{p-4}+2^{p-4}+\ldots+k^{p-4}), \quad \text{mod } p,$$

whence $(-1)^{\frac{1}{2}(p-3)}(\frac{1}{4}-1)\frac{B_{\frac{1}{2}(p-3)}}{-3} \equiv \frac{1}{8}\left(1+\frac{1}{2^3}+\ldots+\frac{1}{k^3}\right)$, mod p;

and therefore

$$(-1)^{\frac{1}{2}(p-3)}B_{\frac{1}{2}(p-3)} \equiv \frac{1}{2}\left(1+\frac{1}{2^3}+\ldots+\frac{1}{k^3}\right), \quad \text{mod } p. \quad \text{(xxiii.)}$$

Similarly, by putting $n = \frac{1}{2}(p-5)$, $n = \frac{1}{2}(p-7)$, ..., we find

$$(-1)^{\frac{1}{2}(p-5)}B_{\frac{1}{2}(p-5)} \equiv \frac{1}{6}\left(1+\frac{1}{2^5}+\ldots+\frac{1}{k^5}\right), \quad \text{mod } p,$$

$$(-1)^{\frac{1}{2}(p-7)}B_{\frac{1}{2}(p-7)} \equiv \frac{1}{18}\left(1+\frac{1}{2^7}+\ldots+\frac{1}{k^7}\right), \quad \text{mod } p,$$

... ...

and, generally, putting $n = \frac{1}{2}(p-2i-1)$,

$$(-1)^{\frac{1}{2}(p-2i-1)}B_{\frac{1}{2}(p-2i-1)} \equiv \frac{2i+1}{2(2^{2i}-1)}\left(1+\frac{1}{2^{2i+1}}+\ldots+\frac{1}{k^{2i+1}}\right), \quad \text{mod } p.$$

The formula which corresponds to the case $n = \frac{1}{2}(p-1)$ is

$$pB_{\frac{1}{2}(p-1)} \equiv (-1)^{\frac{1}{2}(p-1)}, \quad \text{mod } p,$$

which is included in Staudt's theorem.

32. Using the formula

$$\frac{B_n}{2n} \equiv (-1)^{\frac{1}{2}(p-1)}\frac{B_{n-\frac{1}{2}t(p-1)}}{2n-t(p-1)}, \quad \text{mod } p,\text{*}$$

---

* *Messenger*, Vol. XXXII., pp. 63, 129.

to generalize (xxiii.), &c., we have, if p is any Staudt factor for n,

$$(-1)^n pB_n \equiv 1, \text{ mod } p \text{ (Staudt's theorem)};$$

if p is any Staudt factor > 3 for $n+1$,

$$(-1)^n \frac{B_n}{2n} \equiv -\tfrac{1}{6}\left(1+\frac{1}{2^3}+\dots+\frac{1}{k^3}\right), \text{ mod } p;$$

if p is any Staudt factor > 3 for $n+2$,

$$(-1)^n \frac{B_n}{2n} \equiv -\tfrac{1}{30}\left(1+\frac{1}{2^5}+\dots+\frac{1}{k^5}\right), \text{ mod } p;$$

and so on, the general formula being, if p is any Staudt factor >3 for $n+i$, i being $<\frac{1}{2}(p-1)$, then

$$(-1)^n \frac{B_n}{2n} \equiv -\frac{1}{2(2^{2i}-1)}\left(1+\frac{1}{2^{2i+1}}+\dots+\frac{1}{k^{2i+1}}\right), \text{ mod } p.$$

Residue of $(2^{2n}-1)\frac{B_n}{2n}$. (§§ 33–35.)

33. Considering now the form $(2^{2n}-1)\frac{B_n}{2n}$ instead of $\frac{B_n}{2n}$, we notice that for the case $n = \frac{1}{2}(p-1)$ we have

$$\begin{aligned}(2^{p-1}-1)\frac{B_{\frac{1}{2}(p-1)}}{p-1} &\equiv -\frac{2^{p-1}-1}{p}\,pB_{\frac{1}{2}(p-1)}, \text{ mod } p,\\ &\equiv (-1)^{\frac{1}{2}(p+1)}\frac{2^{p-1}-1}{p}, \text{ mod } p,\\ &\equiv (-1)^{\frac{1}{2}(p+1)}\left(1+\frac{1}{3}+\frac{1}{5}+\dots+\frac{1}{p-2}\right), \text{ mod } p,^*\\ &\equiv (-1)^{\frac{1}{2}(p-1)}\frac{1}{2}\left(1+\frac{1}{2}+\dots+\frac{1}{k}\right), \text{ mod } p,\end{aligned}$$

where, as before, $k = \frac{1}{2}(p-1)$.

Thus $$(-1)^{\frac{1}{2}(p-1)}(2^{p-1}-1)\frac{B_{\frac{1}{2}(p-1)}}{p-1} \equiv \frac{1}{2}\left(1+\frac{1}{2}+\dots+\frac{1}{k}\right), \text{ mod } p.$$

---

* *Quarterly Journal*, Vol. xxxii., p. 21.

34. From § 31 we have

$$(-1)^{\frac{1}{2}(p-3)}(2^{p-3}-1)\frac{B_{\frac{1}{2}(p-3)}}{p-3} \equiv \frac{1}{2^3}\left(1+\frac{1}{2^3}+\ldots+\frac{1}{k^3}\right), \text{ mod } p,$$

$$(-1)^{\frac{1}{2}(p-5)}(2^{p-5}-1)\frac{B_{\frac{1}{2}(p-5)}}{p-5} \equiv \frac{1}{2^5}\left(1+\frac{1}{2^5}+\ldots+\frac{1}{k^5}\right), \text{ mod } p,$$

and so on.

35. More generally, if p is any uneven Staudt factor for n,

$$(-1)^n(2^{2n}-1)\frac{B_n}{2n} \equiv \frac{1}{2}\left(1+\frac{1}{2}+\ldots+\frac{1}{k}\right), \text{ mod } p;$$

if p is any uneven Staudt factor for $n+1$,

$$(-1)^n(2^{2n}-1)\frac{B_n}{2n} \equiv \frac{1}{2^3}\left(1+\frac{1}{2^3}+\ldots+\frac{1}{k^3}\right), \text{ mod } p;$$

if p is any uneven Staudt factor for $n+2$,

$$(-1)^n(2^{2n}-1)\frac{B_n}{2n} \equiv \frac{1}{2^5}\left(1+\frac{1}{2^5}+\ldots+\frac{1}{k^5}\right), \text{ mod } p;$$

and so on.

Second Method of obtaining the Residues of E_n, I_n, &c. (§§ 36–43.)

36. The formulæ, (xviii.), (xx.), and (xxii.), which give the residues of E_n, I_n, and $(2^{2n}-1)\frac{B_n}{2n}$ may be obtained very simply by means of the formula

$$x^n+(x-r)^n+(x-2r)^n+\ldots+s^n = r^n\left\{B_{n+1}\left(\frac{x}{r}+1\right)-B_{n+1}\left(\frac{s}{r}\right)\right\},^* \tag{xxiv.}$$

in which x is any number $\equiv s$, mod r.

---

* This formula was given in the *Quarterly Journal*, Vol. XXXI., p. 193, in the form

$$x^n+(x-q)^n+(x-2q)^{2n}+\ldots+r^n = \frac{q^n}{n+1}\left\{V_{n+1}\left(\frac{x}{q}+1\right)-V_{n+1}\left(\frac{r}{q}\right)\right\}.$$

The form in the text is derived by replacing q, r by r, s respectively, and using the relations

$$V_{2n+1}(x) = (2n+1)B_{2n+1}(x), \quad V_{2n}(x) = 2nB_n(x)+(-1)^{n-1}B_n.$$

37. Let $p = kr+t$, t being $< r$. Let $s<r$, and let

$$s' = t-s, \text{ if } s<t,$$

and
$$= r+t-s, \text{ if } s>t \text{ or } = t;$$

so that $s+s' = t$ or $r+t$, according as $s<t$ or $\overline{\overline{<}}\ t$.

Putting $x = p-s'$, the formula (xxiv.) becomes

$$(p-s')^n+(p-s'-r)^n+\ldots+s^n = r^n \left\{ B_{n+1}\left(\frac{p-s'}{r}+1\right)-B_{n+1}\left(\frac{s}{r}\right)\right\}.$$

Now, if $n<p-1$,

$$B_{n+1}\left(\frac{p-s'}{r}+1\right) \equiv B_{n+1}\left(1-\frac{s'}{r}\right), \text{ mod } p ;^*$$

and therefore, writing the terms of the series in the reverse order,

$$s^n+(s+r)^n+(s+2r)^n+\ldots+(p-s')^n$$

$$\equiv r^n \left\{ B_{n+1}\left(\frac{r-s'}{r}\right)-B_{n+1}\left(\frac{s}{r}\right)\right\}, \text{ mod } p.$$

In obtaining this formula n has been supposed to be $<p-1$, but this restriction can be easily removed, so long as $2n$ is not a multiple of $p-1$; for, if $\nu = k(p-1)+n$,

$$s^n \equiv s^{k(p-1)+n} \equiv s^\nu, \text{ mod } p, \quad (s+r)^n \equiv (s+r)^\nu, \text{ mod } p, \text{ \&c.},$$

and
$$B_{n+1}(x) \equiv B_{k(p-1)+n+1}(x) \equiv B_{\nu+1}(x), \text{ mod } p;$$

so that in the formula we may replace n by ν throughout.

38. Since
$$B_{2n+1}(1-x) = -B_{2n+1}(x),$$

and
$$B_{2n}(1-x) = B_{2n}(x),$$

---

* This may be proved as follows. Every term in the expression for $B_n(x)$ in powers of x contains x as a factor, and no term can have p in its denominator unless the Bernoullian number occurring in that term has p as a factor of its denominator. Now the lowest Bernoullian number which has p as a factor of its denominator is $B_{\frac{1}{2}(p-1)}$, and the highest Bernoullian number which occurs in $B_m(x)$ is $B_{\frac{1}{2}(m-1)}$ or $B_{\frac{1}{2}(m-2)}$. If therefore $m<p$, we must have

$$B_m(\alpha p+\beta) \equiv B_m(\beta), \text{ mod } p.$$

we find, by separating the cases in which the exponents are even and uneven,

$$s^{2n}+(s+r)^{2n}+\dots+(p-s')^{2n} \equiv -r^{2n}\left\{B_{2n+1}\left(\frac{s}{r}\right)+B_{2n+1}\left(\frac{s'}{r}\right)\right\}, \bmod p, \tag{xxv.}$$

$$s^{2n-1}+(s+r)^{2n-1}+\dots+(p-s)^{2n-1} \equiv r^{2n-1}\left\{B_{2n}\left(\frac{s'}{r}\right)-B_{2n}\left(\frac{s}{r}\right)\right\}, \bmod p. \tag{xxvi.}$$

In (xxv.) $2n$ must not be a multiple of $p-1$.

39. Put $r=4$, and consider separately the cases of $p=4k+1$ and $p=4k+3$.

(i.) Let $p=4k+1$; then, putting successively $s=1, 2, 3, 4$, so that the corresponding values of s' are $4, 3, 2, 1$, the formula (xxv.) gives

$$\begin{aligned}
1^{2n}+5^{2n}+\dots+(p-4)^{2n} &\equiv -4^{2n}\{B_{2n+1}(\tfrac14)+B_{2n+1}(1)\}, \bmod p,\\
2^{2n}+6^{2n}+\dots+(p-3)^{2n} &\equiv -4^{2n}\{B_{2n+1}(\tfrac12)+B_{2n+1}(\tfrac34)\}, \bmod p,\\
3^{2n}+7^{2n}+\dots+(p-2)^{2n} &\equiv -4^{2n}\{B_{2n+1}(\tfrac34)+B_{2n+1}(\tfrac12)\}, \bmod p,\\
4^{2n}+8^{2n}+\dots+(p-1)^{2n} &\equiv -4^{2n}\{B_{2n+1}(1)+B_{2n+1}(\tfrac14)\}. \bmod p.
\end{aligned}$$

Since $\qquad B_{2n+1}(1)=0, \quad B_{2n+1}(\tfrac12)=0,$

and $\qquad B_{2n+1}(\tfrac34)=-B_{2n+1}(\tfrac14),$

the right-hand members of these four congruences are respectively equal to

$$-4^{2n}B_{2n+1}(\tfrac14), \quad 4^{2n}B_{2n+1}(\tfrac14), \quad 4^{2n}B_{2n+1}(\tfrac14), \quad -4^{2n}B_{2n+1}(\tfrac14).$$

(ii.) Let $p=4k+3$; then, putting as before $s=1, 2, 3, 4$, so that $s'=2, 1, 4, 3$ respectively, (xxv.) gives

$$\begin{aligned}
1^{2n}+5^{2n}+\dots+(p-2)^{2n} &\equiv -4^{2n}\{B_{2n+1}(\tfrac14)+B_{2n+1}(\tfrac12)\}\\
&\equiv -4^{2n}B_{2n+1}(\tfrac14), \bmod p.\\
2^{2n}+6^{2n}+\dots+(p-1)^{2n} &\equiv -4^{2n}\{B_{2n+1}(\tfrac12)+B_{2n+1}(\tfrac14)\}\\
&\equiv -4^{2n}B_{2n+1}(\tfrac14), \bmod p,\\
3^{2n}+7^{2n}+\dots+(p-4)^{2n} &\equiv -4^{2n}\{B_{2n+1}(\tfrac34)+B_{2n+1}(1)\}\\
&\equiv 4^{2n}B_{2n+1}(\tfrac14), \bmod p,\\
4^{2n}+8^{2n}+\dots+(p-3)^{2n} &\equiv -4^{2n}\{B_{2n+1}(1)+B_{2n+1}(\tfrac34)\}\\
&\equiv 4^{2n}B_{2n+1}(\tfrac14), \bmod p.
\end{aligned}$$

These two groups of formulæ include (xviii.) of § 23, and also the results quoted from the *Messenger* in §§ 21 and 22.

40. Put $r = 3$ in (xxv.), and (i.) let $p = 3k+1$. Corresponding to $s = 1, 2, 3$, we have $s' = 3, 2, 1$ respectively, and the formula gives

$$\begin{aligned}
1^{2n}+4^{2n}+\ldots+(p-3)^{2n} &\equiv -3^{2n}\{B_{2n+1}(\tfrac{1}{3})+B_{2n+1}(1)\} \\
&\equiv -3^{2n}B_{2n+1}(\tfrac{1}{3}), \text{ mod } p; \\
2^{2n}+5^{2n}+\ldots+(p-2)^{2n} &\equiv -3^{2n}\{B_{2n+1}(\tfrac{2}{3})+B_{2n+1}(\tfrac{2}{3})\} \\
&\equiv \quad 2\,.\,3^{2n}B_{2n+1}(\tfrac{1}{3}), \quad \text{mod } p; \\
3^{2n}+6^{2n}+\ldots+(p-1)^{2n} &\equiv -3^{2n}\{B_{2n+1}(1)+B_{2n+1}(\tfrac{1}{3})\} \\
&\equiv -3^{2n}B_{2n+1}(\tfrac{1}{3}), \quad \text{mod } p.
\end{aligned}$$

(ii.) Let $p = 3k+2$. Corresponding to $s = 1, 2, 3$, we have $s' = 1, 3, 2$, respectively, and the formula gives

$$\begin{aligned}
1^{2n}+4^{2n}+\ldots+(p-1)^{2n} &\equiv -3^{2n}\{B_{2n+1}(\tfrac{1}{3})+B_{2n+1}(\tfrac{1}{3})\} \\
&\equiv -2\,.\,3^{2n}B_{2n+1}(\tfrac{1}{3}), \text{ mod } p; \\
2^{2n}+5^{2n}+\ldots+(p-3)^{2n} &\equiv -3^{2n}\{B_{2n+1}(\tfrac{2}{3})+B_{2n+1}(1)\} \\
&\equiv \quad 3^{2n}B_{2n+1}(\tfrac{1}{3}), \text{ mod } p; \\
3^{2n}+6^{2n}+\ldots+(p-2)^{2n} &\equiv -3^{2n}\{B_{2n+1}(1)+B_{2n+1}(\tfrac{2}{3})\} \\
&\equiv \quad 3^{2n}B_{2n+1}(\tfrac{1}{3}), \text{ mod } p,
\end{aligned}$$

These groups of formulæ include (xx.), and also the formulæ quoted from the *Messenger*.

In these formulæ and those in the preceding section $2n$ must not be a multiple of $p-1$.

41. Putting $r = 2$ in (xxvi.), we find

$$\begin{aligned}
1^{2n-1}+3^{2n-1}+\ldots+(p-2)^{2n-1} &\equiv \quad 2^{2n-1}\{B_{2n}(1)-B_{2n}(\tfrac{1}{2})\} \\
&\equiv -2^{2n-1}B_{2n}(\tfrac{1}{2}), \text{ mod } p; \\
2^{2n-1}+4^{2n-1}+\ldots+(p-1)^{2n-1} &\equiv \quad 2^{2n-1}\{B_{2n}(\tfrac{1}{2})-B_{2n}(1)\} \\
&\equiv \quad 2^{2n-1}B_{2n}(\tfrac{1}{2}), \text{ mod } p.
\end{aligned}$$

Since $$2^{2n}B_{2n}(\tfrac{1}{2}) = (-1)^n(2^{2n}-1)\frac{B_n}{n},$$

either of these formulæ is equivalent to (xxii.).

42. Put $r=6$ in (xxv.), and let $p=6k+1$. Corresponding to $s=1, 2, 3$,* we have $s'=6, 5, 4$ respectively, and therefore

$$1^{2n}+7^{2n}+\dots+(p-6)^{2n} \equiv -6^{2n}B_{2n+1}(\tfrac{1}{6}), \text{ mod } p;$$

$$2^{2n}+8^{2n}+\dots+(p-5)^{2n} \equiv -6^{2n}\{B_{2n+1}(\tfrac{1}{3})-B_{2n+1}(\tfrac{1}{6})\}, \text{ mod } p;$$

$$3^{2n}+9^{2n}+\dots+(p-4)^{2n} \equiv \quad 6^{2n}B_{2n+1}(\tfrac{1}{3}), \text{ mod } p.$$

Since $\qquad 6^{2n+1}B_{2n+1}(\tfrac{1}{6}) = (-1)^{n+1}\,2\,(2^{2n}+1)\,I_n$

and $\qquad 3^{2n+1}B_{2n+1}(\tfrac{1}{3}) = (-1)^{n+1}I_n,$

these formulæ give

$$1^{2n}+7^{2n}+\dots+(p-6)^{2n} \equiv (-1)^n\,\tfrac{1}{3}\,(2^{2n}+1)\,I_n, \text{ mod } p,$$

$$2^{2n}+8^{2n}+\dots+(p-5)^{2n} \equiv (-1)^n\,\tfrac{1}{3}I_n, \text{ mod } p,$$

$$3^{2n}+9^{2n}+\dots+(p-4)^{2n} \equiv (-1)^{n+1}\,\frac{2^{2n}}{3}I_n, \text{ mod } p.$$

Similarly, for the case $p=6k+5$, by taking $s=1, 2, 5$ to which correspond $s'=4, 3, 6$ respectively, we find

$$1^{2n}+\;7^{2n}+\dots+(p-4)^{2n} \equiv (-1)^n\,\tfrac{1}{3}I_n, \text{ mod } p,$$

$$2^{2n}+\;8^{2n}+\dots+(p-3)^{2n} \equiv (-1)^n\,\frac{2^{2n}}{3}\,I_n, \text{ mod } p,$$

$$5^{2n}+11^{2n}+\dots+(p-6)^{2n} \equiv (-1)^{n+1}\,\tfrac{1}{3}\,(2^{2n}+1)\,I_n, \text{ mod } p.$$

43. From the first formula of the first group and the third formula of the second group, we see, by reversing the order of the terms in the series, that

$$6^{2n}\,(1^{2n}+2^{2n}+\dots+k^{2n}) \equiv \pm(-1)^n\,\tfrac{1}{3}\,(2^{2n}+1)\,I_n, \text{ mod } p,$$

where k is the greatest integer contained in $\dfrac{p}{6}$, and the upper or lower sign is to be taken according as p is of the form $6k+1$ or $6k+5$.

---

* The formulæ corresponding to $s=4, 5, 6$ are not given, as these series are congruent, mod p, to those for $s=3, 2, 1$ respectively, and may be written down at sight by taking the terms in the reverse order, and transforming by

$$(p-t)^{2n} \equiv t^{2n}, \text{ mod } p.$$

Thus the three series reversed give respectively

$$6^{2n}+12^{2n}+\dots+(p-1)^{2n}, \quad 5^{2n}+11^{2n}+\dots+(p-2)^{2n}, \quad 4^{2n}+10^{2n}+\dots+(p-3)^{2n}.$$

A similar remark applies to the case $p=6k+5$, the formulæ for $s=4, 3, 6$ being deducible at sight from those for $s=1, 2, 5$.

Proceeding as in § 28, *i.e.*, by putting $2n = p-3,\ p-5,\ \ldots$, we therefore find that

$$\left.\begin{array}{l} (-1)^{\frac{1}{2}(p-3)} I_{\frac{1}{2}(p-3)} \equiv \pm \dfrac{1}{15}\left(1+\dfrac{1}{2^2}+\ldots+\dfrac{1}{k^2}\right),\ \text{mod}\ p \\ (-1)^{\frac{1}{2}(p-5)} I_{\frac{1}{2}(p-5)} \equiv \pm \dfrac{1}{459}\left(1+\dfrac{1}{2^4}+\ldots+\dfrac{1}{k^4}\right),\ \text{mod}\ p \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \end{array}\right\},\ \text{(xxvii.)}$$

and, in general,

$$(-1)^{\frac{1}{2}(p-2i-1)} I_{\frac{1}{2}(p-2i-1)} \equiv \pm \frac{1}{3^{2i-1}(2^{2i}+1)}\left(1+\frac{1}{2^{2i}}+\ldots+\frac{1}{k^{2i}}\right),\ \text{mod}\ p,$$

where, as before, k is the greatest integer contained in $\frac{p}{6}$, and the upper or lower sign is to be taken according as p is of the form $6k+1$ or $6k+5$.

These results can be generalized as in § 29.

General Formulæ relating to the Residue of $r^{2n+1}B_{2n+1}\left(\frac{s}{r}\right)$, mod p.

(§§ 44–50.)

44. It was shown in § 38 that, $2n$ being any even integer which is not a multiple of $p-1$,

$$s^{2n}+(s+r)^{2n}+\ldots+(p-s')^{2n} \equiv -r^{2n}\left\{B_{2n+1}\left(\frac{s}{r}\right)+B_{2n+1}\left(\frac{s'}{r}\right)\right\},\ \text{mod}\ p,$$

where, if $p = kr+t$, t being $< r$, $s+s' = t$ or $r+t$ according as $s<t$ or $s \overset{=}{>} t$.

For certain values of t and s we may by means of this formula express the residue of $B_{2n+1}\left(\frac{s}{r}\right)$ as a simple sum of powers without the use of μ_1 (§ 19).

45. First, let $t=1$, so that $p = kr+1$; then, by putting $s = 1, 2, 3, \ldots$, we have

$$\begin{aligned} 1^{2n}+(r+1)^{2n}+\ldots+(p-r)^{2n} &\equiv -r^{2n}\left\{B_{2n+1}\left(\frac{1}{r}\right)+B_{2n+1}(1)\right\},\\ &\qquad\qquad \text{mod}\ p,\\ &\equiv -r^{2n}B_{2n+1}\left(\frac{1}{r}\right),\ \text{mod}\ p, \end{aligned}$$

$$2^{2n}+(r+2)^{2n}+\ldots+(p-r+1)^{2n} \equiv -r^{2n}\left\{B_{2n+1}\left(\frac{2}{r}\right)+B_{2n+1}\left(\frac{r-1}{r}\right)\right\}, \quad \text{mod } p,$$

$$\equiv -r^{2n}\left\{B_{2n+1}\left(\frac{2}{r}\right)-B_{2n+1}\left(\frac{1}{r}\right)\right\}, \quad \text{mod } p,$$

$$3^{2n}+(r+3)^{2n}+\ldots+(p-r+2)^{2n} \equiv -r^{2n}\left\{B_{2n+1}\left(\frac{3}{r}\right)+B_{2n+1}\left(\frac{r-2}{r}\right)\right\}, \quad \text{mod } p,$$

$$\equiv -r^{2n}\left\{B_{2n+1}\left(\frac{3}{r}\right)-B_{2n+1}\left(\frac{2}{r}\right)\right\}, \quad \text{mod } p.$$

... ...

$$(r-1)^{2n}+(2r-1)^{2n}+\ldots+(p-2)^{2n} \equiv -r^{2n}\left\{B_{2n+1}\left(\frac{r-1}{r}\right)+B_{2n+1}\left(\frac{2}{r}\right)\right\}, \quad \text{mod } p,$$

$$\equiv -r^{2n}\left\{B_{2n+1}\left(\frac{2}{r}\right)-B_{2n+1}\left(\frac{1}{r}\right)\right\}, \quad \text{mod } p.$$

Thus, in this case of $p = kr+1$, we have

$$-r^{2n}B_{2n+1}\left(\frac{1}{r}\right) \equiv 1^{2n}+(r+1)^{2n}+\ldots+(p-r)^{2n}, \text{ mod } p,$$

$$-r^{2n}B_{2n+1}\left(\frac{2}{r}\right) \equiv (1^{2n}+\ldots)+(2^{2n}+\ldots), \text{ mod } p,$$

$$-r^{2n}B_{2n+1}\left(\frac{3}{r}\right) \equiv (1^{2n}+\ldots)+(2^{2n}+\ldots)+(3^{2n}+\ldots), \text{ mod } p,$$

... ...

and, generally,

$$-r^{2n}B_{2n+1}\left(\frac{s}{r}\right) \equiv (1^{2n}+\ldots)+(2^{2n}+\ldots)+\ldots+(s^{2n}+\ldots), \text{ mod } p.$$

Reversing the order of the terms in the first formula and transforming by $(p-r)^{2n} \equiv r^{2n}$, mod p, &c., we have

$$-r^{2n}B_{2n+1}\left(\frac{1}{r}\right) \equiv r^{2n}\left(1^{2n}+2^{2n}+\ldots+k^{2n}\right), \text{ mod } p.$$

This formula has already been given in § 20.

46. Next, let $p = kr+r-1$. In this case

$$1^{2n}+(r+1)^{2n}+\ldots+(p-r+2)^{2n} \equiv -r^{2n}\left\{B_{2n+1}\left(\frac{1}{r}\right)-B_{2n+1}\left(\frac{2}{r}\right)\right\}, \text{ mod } p,$$

$$2^{2n}+(r+2)^{2n}+\ldots+(p-r+3)^{2n} \equiv -r^{2n}\left\{B_{2n+1}\left(\frac{2}{r}\right)-B_{2n+1}\left(\frac{3}{r}\right)\right\}, \text{ mod } p,$$

... ...

$$(r-2)^{2n}+(2r-2)^{2n}+\ldots+(p-1)^{2n} \equiv -r^{2n}\left\{B_{2n+1}\left(\frac{1}{r}\right)-B_{2n+1}\left(\frac{2}{r}\right)\right\}, \text{ mod } p,$$

$$(r-1)^{2n}+(2r-1)^{2n}+\ldots+(p-r)^{2n} \equiv -r^{2n}\left\{B_{2n+1}\,(1)\,-B_{2n+1}\left(\frac{1}{r}\right)\right\}, \text{ mod } p.$$

Reversing the order of the terms in this last formula, we have

$$r^{2n}B_{2n+1}\left(\frac{1}{r}\right) \equiv r^{2n}+(2r)^{2n}+\ldots+(p-r+1)^{2n}, \text{ mod } p,$$
$$\equiv r^{2n}(1^{2n}+2^{2n}+\ldots+k^{2n}), \text{ mod } p,\text{*}$$

and the other formulæ give

$$r^{2n}B_{2n+1}\left(\frac{2}{r}\right) \equiv (r^{2n}+\ldots)+(1^{2n}+\ldots), \text{ mod } p,$$

$$r^{2n}B_{2n+1}\left(\frac{3}{r}\right) \equiv (r^{2n}+\ldots)+(1^{2n}+\ldots)+(2^{2n}+\ldots), \text{ mod } p,$$

and, generally,

$$r^{2n}B_{2n+1}\left(\frac{s}{r}\right) \equiv (r^{2n}+\ldots)+(1^{2n}+\ldots)+(2^{2n}+\ldots)+\ldots+(s^{2n}+\ldots), \text{ mod } p.$$

47. Now, let $p = kr+2$. In this case

$$1^{2n}+(r+1)^{2n}+\ldots+(p-1)^{2n} \equiv -r^{2n}\left\{B_{2n+1}\left(\frac{1}{r}\right)+B_{2n+1}\left(\frac{1}{r}\right)\right\}, \text{ mod } p,$$

$$2^{2n}+(r+2)^{2n}+\ldots+(p-r)^{2n} \equiv -r^{2n}\left\{B_{2n+1}\left(\frac{2}{r}\right)+B_{2n+1}(1)\right\}, \text{ mod } p,$$

---

* This is the second formula of § 20.

$$3^{2n}+(r+3)^{2n}+\ldots+(p-r+1)^{2n}\equiv -r^{2n}\left\{B_{2n+1}\left(\frac{3}{r}\right)-B_{2n+1}\left(\frac{1}{r}\right)\right\},\quad \text{mod } p,$$

$$4^{2n}+(r+4)^{2n}+\ldots+(p-r+2)^{2n}\equiv -r^{2n}\left\{B_{2n+1}\left(\frac{4}{r}\right)-B_{2n+1}\left(\frac{2}{r}\right)\right\},\quad \text{mod } p,$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$

$$(r-1)^{2n}+(2r-1)^{2n}+\ldots+(p-3)^{2n}$$
$$\equiv -r^{2n}\left\{B_{2n+1}\left(\frac{r-1}{r}\right)-B_{2n+1}\left(\frac{r-3}{r}\right)\right\},\quad \text{mod } p.$$

The first formula gives

$$-2r^{2n}B_{2n}\left(\frac{1}{r}\right)\equiv 1^{2n}+(r+1)^{2n}+\ldots+(p-1)^{2n},\quad \text{mod } p,$$

and the second, reversing the order of the terms, gives

$$r^{2n}B_{2n+1}\left(\frac{2}{r}\right)\equiv r^{2n}\left(1^{2n}+2^{2n}+\ldots+k^{2n}\right),\quad \text{mod } p.$$

From the other formulæ we derive

$$r^{2n}B_{2n+1}\left(\frac{3}{r}\right)\equiv \tfrac{1}{2}\left(1^{2n}+\ldots\right)+\left(3^{2n}+\ldots\right),\quad \text{mod } p,$$

$$r^{2n}B_{2n+1}\left(\frac{4}{r}\right)\equiv \left(r^{2n}+\ldots\right)+\left(4^{2n}+\ldots\right),\quad \text{mod } p.$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$

In this case therefore the formulæ enable us to express the residue of $r^{2n+1}B_{2n+1}\left(\frac{s}{r}\right)$ for all values of s.

48. When $p = kr+r-2$, we obtain similar results, viz.,

$$2r^{2n}B_{2n+1}\left(\frac{1}{r}\right)\equiv (r-1)^{2n}+(2r-1)^{2n}+\ldots+(p-r+1)^{2n},\quad \text{mod } p,$$

$$r^{2n}B_{2n+1}\left(\frac{2}{r}\right)\equiv r^{2n}\left(1^{2n}+2^{2n}+\ldots+k^{2n}\right),\quad \text{mod } p,$$

$$r^{2n}B_{2n+1}\left(\frac{3}{r}\right)\equiv \tfrac{1}{2}\left\{(r-1)^{2n}+\ldots\right\}+\left(1^{2n}+\ldots\right),\quad \text{mod } p,$$

$$r^{2n}B_{2n+1}\left(\frac{4}{r}\right)\equiv \left(r^{2n}+\ldots\right)+\left(2^{2n}+\ldots\right),\quad \text{mod } p,$$

and so on.

49. When $p = kr+3$,

$$1^{2n}+(r+1)^{2n}+\dots+(p-2)^{2n} \equiv -r^{2n}\left\{B_{2n+1}\left(\frac{1}{r}\right)+B_{2n+1}\left(\frac{2}{r}\right)\right\}, \text{ mod } p,$$

$$2^{2n}+(r+2)^{2n}+\dots+(p-1)^{2n} \equiv -r^{2n}\left\{B_{2n+1}\left(\frac{2}{r}\right)+B_{2n+1}\left(\frac{1}{r}\right)\right\}, \text{ mod } p,$$

$$3^{2n}+(r+3)^{2n}+\dots+(p-r)^{2n} \equiv -r^{2n}\left\{B_{2n+1}\left(\frac{3}{r}\right)+B_{2n+1}(1)\right\}, \text{ mod } p,$$

$$4^{2n}+(r+4)^{2n}+\dots+(p-r+1)^{2n} \equiv -r^{2n}\left\{B_{2n+1}\left(\frac{4}{r}\right)-B_{2n+1}\left(\frac{1}{r}\right)\right\}, \text{ mod } p,$$

... ...

$$(r-1)^{2n}+(2r-1)^{2n}+\dots+(p-4)^{2n} \equiv -r^{2n}\left\{B_{2n+1}\left(\frac{4}{r}\right)-B_{2n+1}\left(\frac{1}{r}\right)\right\}, \text{ mod } p.$$

These formulæ do not suffice to assign the residues of $r^{2n}B_{2n+1}\left(\frac{1}{r}\right)$ and $r^{2n}B_{2n+1}\left(\frac{2}{r}\right)$, but only those of $r^{2n}B_{2n+1}\left(\frac{3}{r}\right)$, $r^{2n}B_{2n+1}\left(\frac{6}{r}\right)$, ... ; viz., we have

$$-r^{2n}B_{2n+1}\left(\frac{3}{r}\right) \equiv r^{2n}\left(1^{2n}+2^{2n}+\dots+k^{2n}\right), \text{ mod } p,$$

$$-r^{2n}B_{2n+1}\left(\frac{6}{r}\right) \equiv \left(r^{2n}+\dots\right)+\left(6^{2n}+\dots\right), \text{ mod } p,$$

and so on, as long as the numerators remain $<r$.

If r is uneven, we obtain also the result

$$-2r^{2n}B_{2n}\left(\frac{r+3}{2}\right) \equiv \left(\frac{r+3}{2}\right)^{2n}+\left(\frac{3r+3}{2}\right)^{2n}+\dots+\left(p-\frac{r+3}{2}\right)^{2n}, \text{ mod } p.\text{*}$$

---

* Whenever we obtain the residue of $r^{2n}B_{2n+1}\left(\frac{s}{r}\right)$ it is evident that we obtain also that of $r^{2n}B_{2n+1}\left(\frac{r-s}{r}\right)$, since $B_{2n+1}(1-x) = -B_{2n+1}(x)$.

50. In general, if $p = kr+t$, we have the formulæ:

$$(1) \quad -r^{2n}B_{2n+1}\left(\frac{t}{r}\right) \equiv r^{2n}(1^{2n}+2^{2n}+\ldots+k^{2n}), \text{ mod } p,$$

from which we may derive the residues of

$$r^{2n}B_{2n+1}\left(\frac{2t}{r}\right), \quad r^{2n}B_{2n+1}\left(\frac{3t}{r}\right), \quad \ldots,$$

the numerators being $<r$; (2) if t is even,

$$-2r^{2n}B_{2n+1}\left(\frac{t}{2r}\right) \equiv \left(\frac{t}{2}\right)^{2n}+\left(r+\frac{t}{2}\right)^{2n}+\ldots+\left(p-\frac{t}{2}\right)^{2n}, \text{ mod } p;$$

(3) if t is uneven, and r is uneven,

$$-2r^{2n}B_{2n+1}\left(\frac{r+t}{2r}\right) \equiv \left(\frac{r+t}{2}\right)^{2n}+\left(\frac{3r+t}{2}\right)^{2n}+\ldots+\left(p-\frac{r+t}{2}\right)^{2n}, \text{ mod } p.$$

From (2) and (3) we may obtain other residues as in § 47.

Notes on Isoscelians. By R. Tucker. Received September 7th, 1900. Communicated November 8th, 1900.

1. In Fig. (i.) FG is a positive isoscelian through $P\,(\alpha, \beta, \gamma)$ with reference to the angle A;* then its equation is, if the isoscelian equals r,

$$\begin{vmatrix} \alpha & \beta & \gamma \\ c\,(b-r) & 0 & ar \\ b\,(c-2r\cos A) & 2ar\cos A & 0 \end{vmatrix} = 0,$$

i.e., $$-2r\cos A a\alpha + (c-2r\cos A)\, b\beta + 2\,(b-r)\cos A c\gamma = 0. \qquad \text{(i.)}$$

---

* $+I_A$, $-I_A$ stand for positive and negative isoscelians with reference to angle A respectively.

In Fig. (ii.) DE is a $(-I_A)$ and its equation is

$$-2r\cos A a\alpha + 2\,(c-r)\cos A b\beta + (b-2r\cos A)\,c\gamma = 0. \qquad \text{(ii.)}$$

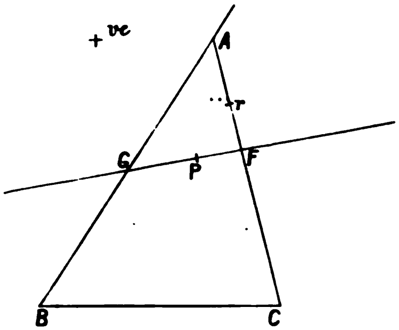


Fig. (i.).

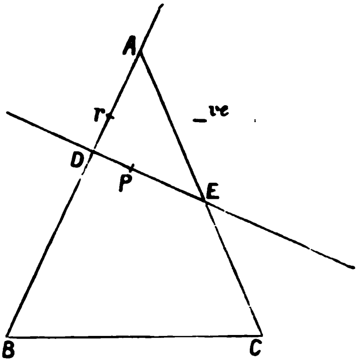


Fig. (ii.).

2. If, now, we draw through P three positive isoscelians (r_1, r_2, r_3), the relation connecting them is found from (i.), viz.,

$$\left.\begin{aligned} -2r_1\cos A a\alpha + (c-2r_1\cos A)\,b\beta + 2\,(b-r_1)\cos A c\gamma &= 0 \\ 2\,(c-r_2)\cos B a\alpha - 2r_2\cos B b\beta + (a-2r_2\cos B)\,c\gamma &= 0 \\ (b-2r_3\cos C)\,a\alpha + 2\,(a-r_3)\cos C b\beta - 2r_3\cos C c\gamma &= 0 \end{aligned}\right\},$$

to be

$$4\,(a^2r_1\cos C\cos A + b^2r_2\cos A\cos B + c^2r_3\cos B\cos C)$$
$$-2\,(abr_1\cos A + bcr_2\cos B + car_3\cos C) - 8\,(car_1 + abr_2 + bcr_3)\,\Pi\cos A$$
$$+abc\,(1+8\Pi\cos A) = 0. \qquad \text{(iii.)}$$

Hence, if $r_1 = r_2 = r_3 = r$, we get the unique solution

$$2r\,(2\Sigma a^2\cos C\cos A - \Sigma ab\cos A - 4\Sigma ab\,\Pi\cos A)$$
$$+abc\,(1+8\Pi\cos A) = 0. \qquad \text{(iv.)}$$

3. For negative isoscelians (iii.) and (iv.) become

$$4\Sigma a^2\rho_1\cos A\cos B - 2\Sigma ca\rho_1\cos A - 8\Pi\cos A\,.\,\Sigma ab\rho_1$$
$$+abc\,(1+8\Pi\cos A) = 0, \qquad \text{(iii. \textit{bis})}$$

and $2\rho\left[2\Sigma a^2\cos A\cos B - \Sigma ca\cos A - 4\Pi\cos A\,.\,\Sigma ab\right]$

$$+abc\,(1+8\Pi\cos A) = 0.^* \qquad \text{(iv. \textit{bis})}$$

---

* Greek letters will indicate negative isoscelians.

4. In Fig. (iv.) take the isoscelians ρ_1, ρ_2, ρ_3; then, if a circle goes through D_1', D_2', &c., we have

$$\rho_2(a-2\rho_3\cos C) = (c-\rho_1)\,2\rho_2\cos B;$$

$$\begin{array}{ll} \text{hence} & \left.\begin{array}{l} 2\rho_1\cos B - 2\rho_3\cos C = c\cos B - b\cos C \\ \text{and also} \quad 2\rho_2\cos C - 2\rho_1\cos A = a\cos C - c\cos A \\ 2\rho_3\cos A - 2\rho_2\cos B = b\cos A - a\cos B \end{array}\right\}. \end{array}$$

Hence $$\Sigma\rho_1 ab\,(a^2-b^2) = 0.$$

Similarly, for positive isoscelians we have

$$\Sigma r_1 ca\,(c^2-a^2) = 0. \qquad \text{(v.)}$$

5. Now the coordinates of D_1', E_1', F_1' are respectively

$$\left.\begin{array}{ccc} 0 & (a-\rho_2)\,c & b\rho_2 \\ c\rho_3 & 0 & (b-\rho_3)\,a \\ (c-\rho_1)\,b & a\rho_1 & 0 \end{array}\right\},$$

and the circle $D_1'E_1'F_1'$ has for its equation

$$P.\Sigma a\beta\gamma = \Sigma a\alpha\left\{\Sigma a\alpha\gamma_1\,(b-\rho_3)\left[a\rho_2^2-(c^2+a^2)\,\rho_2+c\rho_1\rho_2+b\rho_2\rho_3 - ca\rho_1+ac^2\right]\right\}. \qquad \text{(vi.)}$$

If the isoscelians are all $=\rho$, then we have

$$P'.\Sigma a\beta\gamma = \rho\Sigma a\alpha\left\{\Sigma a\alpha\,(b-\rho)\left[(a+b+c)\,\rho^2-(c^2+ac+a^2)\,\rho+ac^2\right]\right\}, \qquad \text{(vi. } bis\text{)}$$

where $$P \equiv abc\left[(a-\rho_2)(b-\rho_3)(c-\rho_1)+\rho_1\rho_2\rho_3\right],$$

and $$P' \equiv abc\left[(a-\rho)(b-\rho)(c-\rho)+\rho^3\right].$$

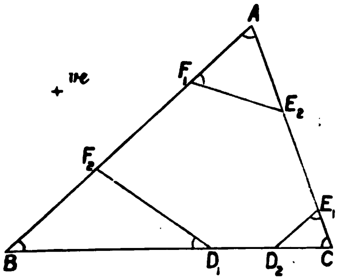


FIG. (iii.).

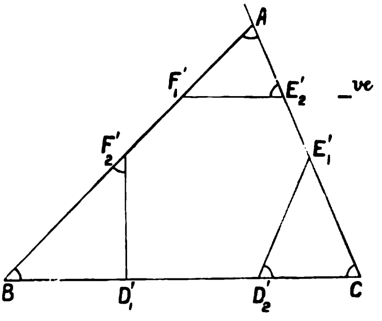


FIG. (iv.).

6. For Fig. (iii.) we have

$$\left.\begin{array}{llll} D_2 & 0 & cr_3 & b(a-r_3) \\ E_2 & c(b-r_1) & 0 & ar_1 \\ F_2 & br_2 & a(c-r_2) & 0 \end{array}\right\},$$

and the circle $D_2E_2F_2$ is

$$Q.\Sigma a\beta\gamma = \Sigma a\alpha\left\{\Sigma a\alpha r_1(c-r_2)\left[ar_3^2-(a^2+b^2)r_3+br_3r_1 \right.\right.$$
$$\left.\left. +cr_2r_3-abr_1+ab^2\right]\right\}, \quad \text{(vii.)}$$

which, in the particular case, becomes

$$Q'.\Sigma a\beta\gamma = r\Sigma a\alpha\left\{\Sigma a\alpha(c-r)\left[(a+b+c)r^2-(a^2+ab+b^2)r+ab^2\right]\right\}, \quad \text{(vii. } bis\text{)}$$

where $Q \equiv abc\left[(a-r_3)(b-r_1)(c-r_2)+r_1r_2r_3\right]$,

$$Q' \equiv abc\left[(a-r)(b-r)(c-r)+r^3\right].$$

7. The radical axis of these circles, when $r = \rho$, is

$$\Sigma a\alpha(b-c)(a^2-\Sigma bc) = 0,$$

which passes through $(b+c)/a$, $(c+a)/b$, $(a+b)/c$.

8. The coordinates of D_1, E_1, F_1 are respectively

$$\begin{array}{ccc} 0 & c(a-2r_2\cos B) & 2br_2\cos B, \\ 2cr_3\cos C & 0 & a(b-2r_3\cos C), \\ b(c-2r_1\cos C) & 2ar_1\cos A & 0. \end{array}$$

Then the circle $D_1E_1F_1$ is

$$R.\Sigma a\beta\gamma = 2\Sigma a\alpha\left\{\Sigma a\alpha r_1\cos A(b-2r_3\cos C)\right.$$
$$\times\left[4ar_2^2\cos^2 B-2(c^2+a^2)r_2\cos B+4br_2r_3\cos B\cos C+4cr_1r_2\cos A\cos B\right.$$
$$\left.\left.-2car_1\cos A+c^2a\right]\right\}, \quad \text{(viii.)}$$

where

$$R \equiv abc\left\{(a-2r_2\cos B)(b-2r_3\cos C)(c-2r_1\cos A)+8r_1r_2r_3\Pi\cos A\right\}.$$

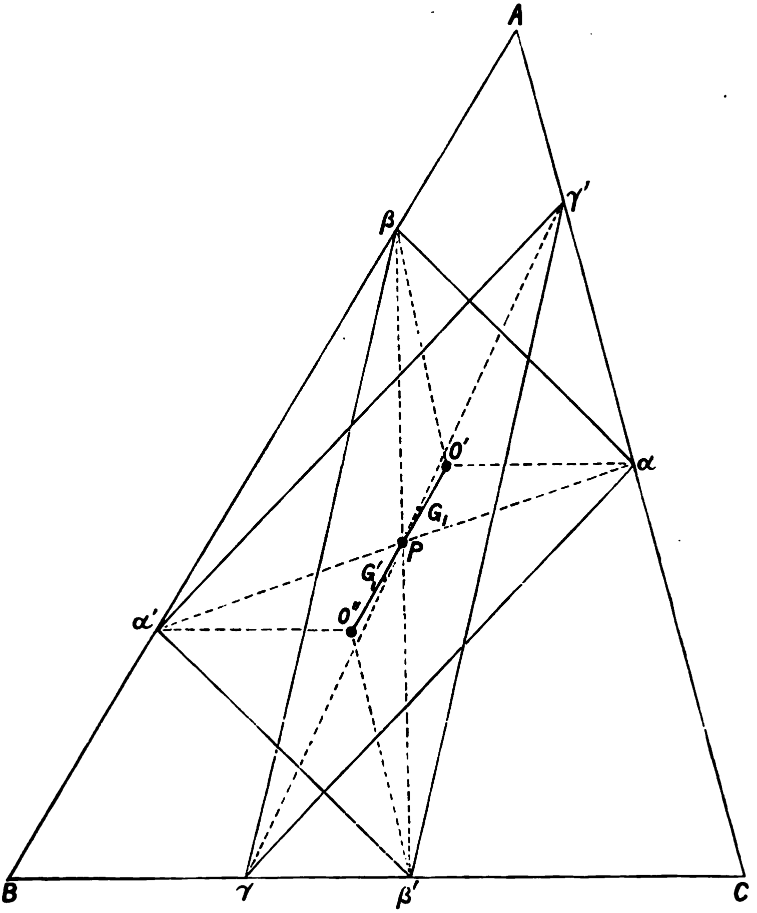
If the isoscelians are equal, the part in [ ] becomes

$$4r^2\cos B(a\cos B+b\cos C+c\cos A)-2r\left\{(c^2+a^2)\cos B+ca\cos A\right\}+c^2a.$$

Two In-Triangles which are similar to the Pedal Triangle.

By R. Tucker. Received September 7th, 1900. Read November 8th, 1900.

1. If ABC is the primitive triangle, then the angles of the pedal triangle are $\pi-2A, \pi-2B, \pi-2C$. The in-triangles, whose sides are anti-parallels, are triangles which are similar to the pedal triangle.



The in-triangles $\alpha\beta\gamma$, $\alpha'\beta'\gamma'$, whose sides are perpendicular to antiparallels, are another pair of similar triangles.

For we have $A\alpha\beta = \frac{\pi}{2} - B$, $A\alpha\gamma = \frac{\pi}{2} - A + C$;

therefore $$\angle\alpha = A\alpha\gamma - A\alpha\beta = \pi - 2A,$$

and so for the other angles.

Again, $B\beta'\alpha' = \frac{\pi}{2} - A$, $B\beta'\gamma' = \frac{\pi}{2} - B + C$;

therefore $$\angle\beta' = \pi - 2B,$$

and so for the other angles.

Hence $\alpha\beta\gamma$, $\alpha'\beta'\gamma'$ are similar to the pedal triangle.

2. If λ be a constant to be determined, and if, for brevity, we write p, q, r for $\sin 2A$, $\sin 2B$, $\sin 2C$, we have

$$B\gamma \sin B = \lambda . p \cos C \quad \text{and} \quad C\gamma \sin C = \lambda . q \cos (C-A),$$

then $$2a \sin B \sin C = 2\lambda \left[p \sin C \cos C + q \sin B \cos (C-A) \right]$$
$$= \lambda . \Sigma (qr) = 2\lambda \left[\Pi \cos A + \Pi \cos (B-C) \right],$$

and $$\lambda = 4R . \Pi \sin A / \Sigma (qr). \qquad \text{(i.)}$$

If λ' corresponds to λ, then

$$B\beta' \sin B + C\beta' \sin C = \lambda' \left[r \cos (A-B) + p \cos B \right],$$

whence, as before, $\lambda' = 4R . \Pi \sin A / \Sigma (qr) = \lambda$,

i.e., $\alpha\beta\gamma$, $\alpha'\beta'\gamma'$ are congruent.

3. Now $$\beta'\gamma = B\beta' - B\gamma = \lambda \left[r \cos (A-B) - p \cos C \right] / \sin B$$
$$= \lambda \cos C . q / \sin B = 2\lambda \cos B \cos C \propto \sec A.$$

4. Using trilinear coordinates, we have

$$\left.\begin{array}{llll}
(\alpha) & q \cos A & 0 & r \cos (A-B) \\
(\beta) & p \cos (B-C) & r \cos B & 0 \\
(\gamma) & 0 & q \cos (C-A) & p \cos C \\
(\alpha') & r \cos A & q \cos (C-A) & 0 \\
(\beta') & 0 & p \cos B & r \cos (A-B) \\
(\gamma') & p \cos (B-C) & 0 & q \cos C
\end{array}\right\} . \qquad \text{(ii.)}$$

5. The lines $\alpha\alpha'$, $\beta\beta'$ are

$$-qr\cos(A-B)\cos(C-A)\,\alpha+r^2\cos A\cos(A-B)\,\beta$$
$$+q^2\cos A\cos(C-A)\,\gamma=0,$$

$$r^2\cos B\cos(A-B)\,\alpha-rp\cos(B-C)\cos(A-B)\,\beta$$
$$+p^2\cos B\cos(B-C)\,\gamma=0;$$

hence $\alpha\alpha'$, $\beta\beta'$, $\gamma\gamma'$ cointersect in P, the centre of similitude* of the triangles, given by

$$\alpha/p\cos(B-C)=\ldots=\ldots. \qquad \text{(iii.)}$$

6. The equations to $\alpha\beta$, $\gamma'\alpha'$ are respectively

$$-r\cos B\cos(A-B)\,\alpha+p\cos(A-B)\cos(B-C)\,\beta+q\cos A\cos B\,.\,\gamma=0, \qquad \text{(iv.)}$$

$$-q\cos C\cos(C-A)\,\alpha+r\cos A\cos C\,\beta+p\cos(B-C)\cos(C-A)\,\gamma=0. \qquad \text{(v.)}$$

Let their point of intersection be P' (Q', R' for the analogous pairs); then AP', BQ', CR' meet in

$$\alpha/\cos(B-C),\ \ldots,\ \ldots,\ \textit{i.e.},\ \text{in the nine-point centre.} \qquad \text{(vi.)}$$

7. The equations to $\alpha'\beta'$, $\gamma\alpha$ are

$$q\cos(A-B)\cos(C-A)\,\alpha-r\cos A\cos(A-B)\,\beta+p\cos A\cos B\,.\,\gamma=0, \qquad \text{(vii.)}$$

$$r\cos(C-A)\cos(A-B)\,\alpha+p\cos C\cos A\,.\,\beta-q\cos A\cos(C-A)\,\gamma=0. \qquad \text{(viii.)}$$

Let their point of intersection be P'' (Q'', R'' for the analogous pairs); then AP'', BQ'', CR'' meet in

$$\alpha/\cos A=\ldots=\ldots,\ \textit{i.e.},\ \text{in the circumcentre.} \qquad \text{(ix.)}$$

---

* [Many of the geometrical results follow at once from this fact, but the equations to the lines and points are given, as they may suggest other properties. Further, P is the P' of my paper "On a Group of Triangles inscribed in a given Triangle *ABC*, &c.," Vol. XXIV., pp. 131-142, whence other properties can be derived than those given in the present paper.]

8. The centroids of $\alpha\beta\gamma$, $\alpha'\beta'\gamma'$ respectively are given by

$$\left.\begin{array}{ll} & \alpha/\cos A\,(2q+r) = \ldots = \ldots \quad (G_1) \\ \text{and} & \alpha/\cos A\,(q+2r) = \ldots = \ldots \quad (G_1') \end{array}\right\}; \qquad \text{(x.)}$$

therefore their join is given by the equation

$$\Sigma \cos B \cos C\,(qr-p^2)\,\alpha = 0, \qquad \text{(xi.)}$$

and this passes through $(q+r)\cos A, \ldots, \ldots$, *i.e.*, through $p\cos(B-C)$, $\ldots, \ldots$, *i.e.*, the point P [*cf.* (iii.)].

9. If O', O'' are the in-centres of $\alpha\beta\gamma$, $\alpha'\beta'\gamma'$ respectively, then, since

$$\angle C\alpha O' = C\alpha\gamma + \gamma\alpha O' = \left(\frac{\pi}{2} - C + A\right) + \left(\frac{\pi}{2} - A\right) = \pi - C,$$

$\alpha O'$ is parallel to BC, and similarly $\beta O'$ is parallel to CA, and $\gamma O'$ is parallel to AB.

In like manner, $\alpha' O''$, $\beta' O''$, $\gamma' O''$ are respectively parallel to BC, CA, AB. Hence their coordinates are given by

$$\left.\begin{array}{ll} & q\cos A, \ r\cos B, \ p\cos C \\ \text{and} & r\cos A, \ p\cos B, \ q\cos C \end{array}\right\}. \qquad \text{(xii.)}$$

Hence the equation to $O'O''$ is

$$\Sigma \alpha \cos B \cos C\,(qr-p^2) = 0, \ \ldots \ [\textit{cf.}\ \text{(xi.)}],$$

and the mid-point of $O'O''$ is P (iii.).

10. The symmedian line through α [*cf.* (iv.) and (viii.)] is

$$-r\cos B\cos(A-B)\,\alpha + p\cos(A-B)\cos(B-C)\,\beta + q\cos A\cos B\,.\,\gamma$$
$$= \lambda\left[r\cos(C-A)\cos(A-B)\,\alpha + p\cos C\cos A\,.\,\beta - q\cos A\cos(C-A)\,\gamma\right].$$

If, for the moment, this line cuts $\beta\gamma$ in D, then

$$\beta D : D\gamma = r^2 : q^2;$$

hence, from (ii.), we get the coordinates of D to be proportional to

$$pq^2\cos(B-C), \quad q^2 r\cos B + qr^2\cos(C-A), \quad r^2 p\cos C.$$

Substituting in the above equation to αD, we get, after dividing by $S\,[\equiv \Sigma\,(qr)]$,

$$\lambda r = -q;$$

and the equation to αD becomes

$$\begin{aligned}\alpha r\cos(A-B)&\left[r\cos(C-A)+q\cos B\right]\\ &+\beta p\left[r\cos C\cos A-q\cos(A-B)\cos(B-C)\right]\\ &-\gamma q\cos A\left[q\cos B+r\cos(C-A)\right]=0.\end{aligned}\qquad\text{(xiii.)}$$

The symmedian through β then is

$$\begin{aligned}-\alpha r\cos B&\left[r\cos C+p\cos(A-B)\right]\\ &+\beta p\cos(B-C)\left[p\cos(A-B)+r\cos C\right]\\ &+\gamma q\left[p\cos A\cos B-r\cos(B-C)\cos(C-A)\right]=0.\end{aligned}$$

Hence the symmedian point of $\alpha\beta\gamma$ is

$$pq\left[p\cos A+q\cos(B-C)\right],\ \ldots,\ \ldots;\qquad\text{(xiv.)}$$

and similarly of $\alpha'\beta'\gamma'$ is

$$rp\left[p\cos A+r\cos(B-C)\right],\ \ldots,\ \ldots.$$

11. Drawing αX, perpendicular to $\beta\gamma$, to meet it in X (*i.e.*, parallel to an anti-parallel), we get X given by

$$q\cos 2C\cos(B-C),\quad -qr\sin B,\quad r\cos 2B\cos 2C;$$

and from α and X we can find the coordinates of H_1 (the orthocentre of $\alpha\beta\gamma$) to be

$$\left.\begin{array}{l}\qquad\qquad a\cos 2C,\quad b\cos 2A,\quad c\cos 2B;\\ \text{similarly } H_2 \text{ (for } \alpha'\beta'\gamma'\text{) is given by}\\ \qquad\qquad a\cos 2B,\quad b\cos 2C,\quad c\cos 2A.\end{array}\right\}\qquad\text{(xv.)}$$

Hence the equation to H_1H_2 is

$$\Sigma bc\alpha\left(\cos^2 2A-\cos 2B\cos 2C\right)=0,\qquad\text{(xvi.)}$$

a line which passes through P.

12. The circles $\alpha\beta\gamma$, $\alpha'\beta'\gamma$ are given by

$$\left.\begin{array}{l}S^2.\Sigma\alpha\beta\gamma=2\Sigma a\alpha\left[\Sigma qr\sin C\cos(A-B)\sin(2C-A)\,\alpha\right]\\ S^2.\Sigma\alpha\beta\gamma=2\Sigma a\alpha\left[\Sigma qr\sin B\cos(C-A)\sin(2B-A)\,\alpha\right]\\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad(cf.\ \S\,10)\end{array}\right\}.\qquad\text{(xvii.)}$$

Their radical axis is

$$\Sigma\left[\alpha qr\sin A\sin(B-C)(\cos 3A-2\cos B\cos C)\right]=0,\qquad\text{(xviii.)}$$

and it passes through the circumcentre.

13. The circles $C\beta'\gamma'$, $A\gamma'\alpha'$ have for equations

$$S.\Sigma a\beta\gamma = 2\Sigma a\alpha\left[p\sin B\alpha+(p+q)\sin A\beta\right]\cos C, \qquad \text{(xix.)}$$

$$S.\Sigma a\beta\gamma = 2\Sigma a\alpha\left[q\sin C\beta+(q+r)\sin B\gamma\right]\cos A; \qquad \text{(xx.)}$$

and the circles $B\beta\gamma$, $C\gamma\alpha$ are given by

$$S.\Sigma a\beta\gamma = 2\Sigma a\alpha\left[r\sin C\alpha+(r+p)\sin A\gamma\right]\cos B, \qquad \text{(xxi.)}$$

$$S.\Sigma a\beta\gamma = 2\Sigma a\alpha\left[p\sin A\beta+(p+q)\sin B\alpha\right]\cos C. \qquad \text{(xxii.)}$$

Hence the radical axis of $C\beta'\gamma'$ and $C\gamma\alpha$ is

$$\alpha/a = \beta/b;$$

and therefore it, and the analogous radical axes, pass through K, the symmedian point of ABC.

14. From the above we see that the radical axis of the circles $B\beta\gamma$, $C\beta'\gamma'$ is

$$\alpha\left[p\sin B\cos C - r\sin C\cos B\right] + \left[\beta(p+q)\cos C-\gamma(r+p)\cos B\right]\sin A = 0; \qquad \text{(xxiii.)}$$

hence, if it cuts BC in L, and the analogous radical axes cut CA, AB in M, N respectively, then these axes meet in P.

15. The circles $A\alpha\alpha'$, $B\beta\beta'$, $C\gamma\gamma'$ have their equations

$$S.\Sigma a\beta\gamma = \Sigma a\alpha\,(cr\beta+bq\gamma)\cos A, \qquad \text{(xxiv.)}$$

$$S.\Sigma a\beta\gamma = \Sigma a\alpha\,(ap\gamma+cr\alpha)\cos B, \qquad \text{(xxv.)}$$

$$S.\Sigma a\beta\gamma = \Sigma a\alpha\,(bq\alpha+ap\beta)\cos C. \qquad \text{(xxvi.)}$$

The radical axis of (xxiv.) and (xxv.) is

$$cr\,(\alpha\cos B-\beta\cos A)+(ap\cos B-bq\cos A)\,\gamma = 0.$$

If this cuts AB in N' (and L', M' are analogous points), then AL', BM', CN' pass through the circumcentre.

16. The equation to the conic through the six points is

$$\Sigma\left[qr\alpha^2/\cos A\cos(B-C)\right] = \Sigma\left[(S+2p^2)\,\beta\gamma/\cos(C-A)\cos(A-B)\right]. \qquad \text{(xxvii.)}$$

17. It may be noted that

$$\left.\begin{aligned} \angle A\alpha\beta &= \frac{\pi}{2} - B = C\gamma'\beta' \\ \angle B\beta\gamma &= \frac{\pi}{2} - C = A\alpha'\gamma' \\ \angle C\gamma\alpha &= \frac{\pi}{2} - A = B\beta'\alpha' \end{aligned}\right\}.$$

18. To construct the figure, let DEF be the pedal triangle; then its sides are Rp, Rq, Rr.

If DK, EL, FM are the perpendiculars of DEF, then

$$DK = Rqr, \quad EL = Rrp, \quad FM = Rpq. \qquad (a)$$

Now

$$\begin{aligned} \lambda &= 4R\Pi\,(\sin A)/\Sigma\,(qr), \\ &= R\,(p+q+r)/\Sigma\,(qr), \\ &= R\,\frac{DE+EF+FD}{DK+EL+FM}. \end{aligned}$$

Hence the sides of $\alpha\beta\gamma$, $\alpha'\beta'\gamma'$ (*i.e.*, $\lambda.Rp$, $\lambda.Rq$, $\lambda.Rr$) are known.

[I am indebted to a referee for a suggestion which enables me to considerably simplify the construction, viz.,

$$B\gamma' : \gamma\beta' : \beta'C = \operatorname{cosec} 2B : \operatorname{cosec} 2A : \operatorname{cosec} 2C,$$

i.e., by (a),

$$= EL : FM : DK.]$$

On Quantitative Substitutional Analysis. By A. YOUNG.

Communicated November 8th, 1900. Received November 9th, 1900. Received, in revised form, January 12th, 1901.

From any function P of n variables may be obtained $n!$ functions, not necessarily all different, by permuting the variables in P in all possible ways; or, what is the same thing, by operating on P with each of the $n!$ substitutions of the symmetric group of the variables. It frequently happens that between these functions linear relations with constant coefficients exist; such may be written

$$(\lambda_1+\lambda_2 s_2+\lambda_3 s_3+\ldots)\,P = 0,$$

$\lambda_1, \lambda_2, \ldots$ being numbers positive or negative, integral or fractional, and $s_2, s_3, \ldots$ substitutions belonging to the symmetric group of the variables. The words "substitutional relation" will be used to denote a relation such as that just written down; and the expression "substitutional equation" will be used for the same relation when P is an unknown function for which this relation is true. The simplest form of such a relation is

$$(1-s)\,P=0,$$

which merely implies that P is unaltered by the substitution s. This is dealt with in the theory of substitutions. The main object of the present paper is the discussion of single equations, such as that written down above, or of simultaneous systems of such equations, with a view to their solution; further, of the discussion of equations of the form

$$(\lambda_1+\lambda_2 s_2+\lambda_3 s_3+\ldots)\,P=R,$$

where $\lambda_1, \lambda_2, \ldots, s_2, s_3, \ldots$ are defined as above, and R is a known function; these equations are also to be included in the term "substitutional equations." It will be seen, moreover, that the right-hand sides of such equations, when a single equation, or else a simultaneous system, is under consideration, are subject to restrictions, in that they have in general to satisfy certain substitutional relations.

The problem proposed is not a purely hypothetical one. In a paper on "The Irreducible Concomitants of any Number of Binary Quartics,"* I have shown that there is one type of concomitant to be discussed for each degree and order; and that such a type satisfies certain substitutional equations, the solution of which enables us to find how many concomitants of that type for a definite number of quartics are irreducible, and which these are. The equations were there discussed, and the irreducible system for any number of quartics was found. Thus, using the notation of that paper, the invariant type degree 6 may be written $(abcdef)$; it satisfies the equations

$$(abcdef)=(bcdefa)=(afedcb),$$

$$(abcdef)+(abcfde)+(abcefd)+(abcdfe)+(abcfed)+(abcedf)=R,$$

$$(abcdef)+(abfcde)+(abefcd)+(abcdfe)+(abecdf)+(abfecd)=R,$$

where R stands for certain reducible terms, with the form of which we are not concerned. The other equations satisfied by this type are a necessary consequence of the four written down.

---

* *Proc. Lond. Math. Soc.*, Vol. xxx., p. 290.

Later, in a paper on "The Invariant Syzygies of Lowest Degree for any Number of Quartics,"* I proved that the substitutional equations satisfied by the quartic types gave all the syzygies between quartic concomitants; but here the form of the reducible terms on the right-hand sides of the equations had to be included in the discussion. The equations for invariant types up to and including degree 7 were discussed, with the result that no invariant syzygies existed of degree less than 7, and that the syzygies of degree 7 could all be obtained from one definite form. Incidentally, the method of discussing the equations with a view simply to finding the irreducible system was somewhat improved; and a theorem connected with substitutional analysis was proved, which has been generalized here, § 8.

The term "substitutional expression" is used to denote an expression of the form

$$\lambda_1+\lambda_2 s_2+\lambda_3 s_3+\ldots+\lambda_p s_p,$$

where $\lambda_1, \lambda_2, \ldots$ are numerical constants (positive or negative) and $s_2, s_3, \ldots$ are substitutions. It is shown, to start with, that the solution of substitutional equations, so far as rational integral algebraic functions are concerned, may be made to depend on the finding of substitutional expressions which satisfy the equations in virtue of the multiplication table of the group to which all the substitutions belong. The first seven paragraphs of this paper are concerned with substitutional equations; in § 9 some examples are given.

The second part of the paper has to do with two substitutional identities, one of which is proved in § 13, the other in § 15. By means of relations which are established between substitutional and polar operations on functions of a definite kind, from the first of these a proof of Gordon's series is obtained; from the second Capelli's extension of this series, a theorem due to Peano, and some corollaries concerning substitutional equations. An account of the paper which contains Capelli's theorem is also given, § 11, as there exists a fairly close connexion between the analysis of substitutional and polar operators. With this connexion § 12 has to do; it is somewhat further developed in that part of § 17 which has to do with Capelli's theorem.

For convenience, owing to the quantitative use of the symbols, the substitutions next a function are regarded as operating on it before those further away, thus

---

* *Proc. Lond. Math. Soc.*, Vol. XXXII., p. 384.

$$s_1 s_2 P = s_1 (s_2 P).$$

To avoid confusion, as the symbol (*abc*...) is used in two senses, viz., as a substitution and as a concomitant type of a quantic, Roman letters are used when it denotes a substitution, italics when it denotes a type. The usual symbols for a group are used in two senses: first, as a name for the group, and; secondly, to represent the sum of the substitutions of the group. The following notation is made use of:—

$\{s\}$ = the sum of the substitutions of the smallest group including s.

$\{s_1, s_2\}$ = the sum of the substitutions of the smallest group including s_1 and s_2.

$\{G_1, G_2\}$ = the sum of the substitutions of the smallest group having G_1 and G_2 for sub-groups.

$\{\mathrm{abc}\ldots\}$ = the symmetric group of the letters $a, b, c, \ldots$

$\{\mathrm{abc}\ldots\}'$ = the sum of the substitutions of the alternating group of the letters $a, b, c, \ldots$, minus the substitutions of these letters which do not belong to the alternating group.

The expression $\{\mathrm{abc}\ldots\}$ is sometimes referred to as "the positive symmetric group"; while $\{\mathrm{abc}\ldots\}'$ is called "the negative symmetric group."

The paper has been rewritten and greatly enlarged at the request of the referees; my thanks are due to them—particularly to Prof. Burnside—for many valuable criticisms and suggestions.

1. Consider any rational integral algebraic function P of n variables $a_1, a_2, \ldots, a_n$; its terms may be arranged in sets $P_1, P_2, \ldots, P_m$, such that each set contains all those terms of P, and only those, which are obtainable from some particular term by means of substitutions and of positive or negative numerical factors. And P may be written

$$P = P_1 + P_2 + \ldots + P_m.$$

Now, consider any set P_1; let $A_1 a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n}$ be any term of this set, A_1 being a positive or negative numerical coefficient; then

$$P_1 = (A_1 + A_2 s_2 + A_3 s_3 + \ldots)\, a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n},$$

where $A_1, A_2, \ldots$ are numerical, and $s_2, s_3, \ldots$ substitutions belonging to the symmetric group of the n variables. The effects of substitutions on P_1, and consequently all substitutional properties of P_1, depend partly on the substitutional operator $(A_1 + A_2 s_2 + A_3 s_3 + \dots)$, partly on the substitutional properties of the term $a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n}$. If in this term all the indices $\alpha_1, \alpha_2, \dots, \alpha_n$ are different, we obtain by operating on it with the $n!$ substitutions of the symmetric group $\{\mathrm{a}_1 \mathrm{a}_2 \dots \mathrm{a}_n\}$ of the variables $n!$ different terms which are connected by no linear relations with constant coefficients. In this case, then, $a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n}$ has no substitutional properties, and all the substitutional properties of P_1 are a consequence of the operator

$$(A_1 + A_2 s_2 + A_3 s_3 + \dots).$$

Suppose next that $\alpha_1 = \alpha_2 = \dots = \alpha_r = \alpha$, and that $\alpha, \alpha_{r+1}, \alpha_{r+2}, \dots, \alpha_n$ are all different. The substitutional properties of the term

$$a_1^{\alpha} a_2^{\alpha} \dots a_r^{\alpha} a_{r+1}^{\alpha_{r+1}} a_{r+2}^{\alpha_{r+2}} \dots a_n^{\alpha_n}$$

consist solely of the fact that this term belongs to the group $\{\mathrm{a}_1 \mathrm{a}_2 \dots \mathrm{a}_r\}$. For there result, by operating on it with the $n!$ substitutions of the group $\{\mathrm{a}_1 \mathrm{a}_2 \dots \mathrm{a}_n\}$, $\frac{n!}{r!}$ different terms between which no linear relations with constant coefficients can exist. The substitutional properties of this term are then identical with those of

$$\{\mathrm{a}_1 \mathrm{a}_2 \dots \mathrm{a}_r\}\, a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n},$$

where all the indices of the a's in $a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n}$ are different. Hence all the substitutional properties of P_1 are, in this case, a consequence of the operator when we write, as may be done,

$$P_1 = \frac{1}{r!} \left[(A_1 + A_2 s_2 + A_3 s_3 + \dots) \{\mathrm{a}_1 \mathrm{a}_2 \dots \mathrm{a}_r\} \right] a_1^{\alpha} a_2^{\alpha} \dots a_r^{\alpha} a_{r+1}^{\alpha_{r+1}} a_{r+2}^{\alpha_{r+2}} \dots a_n^{\alpha_n}$$

$$= (B_1 + B_2 s_2 + B_3 s_3 + \dots)\, a_1^{\alpha} a_2^{\alpha} \dots a_r^{\alpha} a_{r+1}^{\alpha_{r+1}} a_{r+2}^{\alpha_{r+2}} \dots a_n^{\alpha_n},$$

where

$$\frac{1}{r!} (A_1 + A_2 s_2 + A_3 s_3 + \dots) \{\mathrm{a}_1 \mathrm{a}_2 \dots \mathrm{a}_r\} = (B_1 + B_2 s_2 + B_3 s_3 + \dots),$$

the B's being constants. In exactly the same way, whatever be the equalities amongst the indices in the term $a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n}$, a substitutional operator $(B_1 + B_2 s_2 + B_3 s_3 + \dots)$ may be obtained, such that

$$P_1 = (B_1 + B_2 s_2 + B_3 s_3 + \dots)\, a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n},$$

all the substitutional properties of P_1 being a consequence of the operator alone.

Now, owing to the way in which the sets have been chosen, no substitution can change a term of one set into a term of a different set; and there can exist no substitutional relation between different sets. Hence, if P satisfy any substitutional equation

$$(\lambda_1+\lambda_2 s_2+\lambda_3 s_3+\ldots)\,P=0,$$

where $\lambda_1, \lambda_2, \ldots$ are constants, each set must independently satisfy this equation. And hence each set possesses all the substitutional properties of P.

Theorem.—Every rational integral algebraic function P of n variables may be written in the form $P=\sum_{i=1}^{i=m} P_i$, where P_i possesses all the substitutional properties of P, and possibly others as well. And P_i may be expressed in the form

$$P_i=(A_1^{(i)}+A_2^{(i)}s_2+A_3^{(i)}s_3+\ldots)\,F_i,$$

where $A_1^{(i)}, A_2^{(i)}, \ldots$ are positive or negative numerical coefficients, $s_2, s_3, \ldots$ are substitutions belonging to the symmetric group of the n variables, and F_i is a rational integral algebraic function of the variables. Further, the substitutional operator

$$(A_1^{(i)}+A_2^{(i)}s_2+A_3^{(i)}s_3+\ldots)$$

is such that all the substitutional properties of P_i are a direct consequence of it.

For example, take the form

$$P=\tfrac{1}{2}a_2-\tfrac{1}{2}a_3+3a_1^2a_2-\tfrac{1}{5}a_2^2a_3-3a_1^2a_3+\tfrac{1}{5}a_2a_3^2;$$

then
$$P_1=\tfrac{1}{2}a_2-\tfrac{1}{2}a_3=\tfrac{1}{2}\{\mathrm{a}_2\mathrm{a}_3\}'\,a_2=\tfrac{1}{4}\{\mathrm{a}_2\mathrm{a}_3\}'\,\{\mathrm{a}_1\mathrm{a}_3\}\,a_2$$
$$=\tfrac{1}{4}\left[1-(\mathrm{a}_2\mathrm{a}_3)+(\mathrm{a}_1\mathrm{a}_3)-(\mathrm{a}_1\mathrm{a}_2\mathrm{a}_3)\right]a_2,$$
$$P_2=3a_1^2a_2-\tfrac{1}{5}a_2^2a_3-3a_1^2a_3+\tfrac{1}{5}a_2a_3^2$$
$$=\left[3-\tfrac{1}{5}(\mathrm{a}_1\mathrm{a}_2\mathrm{a}_3)-3(\mathrm{a}_2\mathrm{a}_3)+\tfrac{1}{5}(\mathrm{a}_1\mathrm{a}_3)\right]a_1^2a_2,$$
$$P=P_1+P_2.$$

Here P, P_1, P_2 all satisfy the equation

$$\{\mathrm{a}_2\mathrm{a}_3\}\,P=0;$$

also P_1 satisfies the equation

$$\{a_1 a_2 a_3\}' P_1 = 0.$$

Again, if the substitutional properties of P are completely summed up by saying that P belongs to the group G of order ρ, it is sufficient and more convenient to write

$$P = \frac{1}{\rho} GP,$$

this being, as it is easy to verify, the necessary and sufficient condition that P may belong to the group G of order ρ.

Corollary.—Every rational integral algebraic solution P of a single equation

$$(\lambda_1 + \lambda_2 s_2 + \lambda_3 s_3 + \ldots) P = 0,$$

where λ_1, λ_2, ... are constants, and s_2, s_3, ... substitutions belonging to the symmetric group of the variables, of which P is supposed to be a function, or of a simultaneous system of such equations, may be obtained in the form

$$P = \sum_i (A_1^{(i)} + A_2^{(i)} s_2 + A_3^{(i)} s_3 + \ldots) F_i ;$$

where $A_1^{(i)}$, $A^{(i)}$, ... are constants, and F_i is a rational integral algebraic function of the variables, the substitutional operator of each term being such that

$$(\lambda_1 + \lambda_2 s_2 + \lambda_3 s_3 + \ldots)(A_1^{(i)} + A_2^{(i)} s_2 + A_3^{(i)} s_3 + \ldots) \equiv 0,$$

in virtue of the multiplication table of the group.

For P may be written in the form

$$P = \sum_i P_i,$$

where
$$P_i = (A_1^{(i)} + A_2^{(i)} s_2 + \ldots) F_i,$$

all the substitutional properties of P_i being consequences of the operator, and, further, where P_i possesses all the substitutional properties of P, and hence is a solution of the equation, or system of equations, of which we are supposing P to be a solution. But, since every substitutional property of P_i is a consequence of the operator $(A_1^{(i)} + A_2^{(i)} s_2 + \ldots)$, it follows that

$$(\lambda_1 + \lambda_2 s_2 + \ldots)(A_1^{(i)} + A_2^{(i)} s_2 + \ldots) \equiv 0.$$

2. The applications of our theory at present required are entirely to functions rational integral algebraic in the variables. Consequently,

we may restrict ourselves to the discussion of such functions, and will throughout this paper tacitly assume that the functions considered are of this nature. Nevertheless, should the theorem of the preceding article be true for any kind of function—as seems to me probable—no restrictions as to the nature of the functions considered would be necessary.

In consequence of the corollary just proved, it follows that in order to obtain the solutions of a system of equations of the form

$$(\lambda_1+\lambda_2 s_2+\lambda_3 s_3+\ldots)\,P=0$$

it is only necessary to discover the substitutional expressions

$$(A_1+A_2 s_2+A_3 s_3\ldots)$$

which are such that

$$(\lambda_1+\lambda_2 s_2+\lambda_3 s_3+\ldots)(A_1+A_2 s_2+A_3 s_3+\ldots)\equiv 0,$$

in virtue of the multiplication table of the group. The solution is then a matter of relations between substitutional operators only. We may then proceed thus: Take the sum of all the substitutions of the group concerned with arbitrary coefficients; for brevity we write this S. Then expand the various expressions

$$(\lambda_1+\lambda_2 s_2+\ldots)\,S$$

obtained by substituting S for P in the various equations of the simultaneous system, and in the results equate the coefficient of each substitution to zero. A system of simultaneous linear equations is thus obtained for the arbitrary constants in S. As a rule, all the arbitrary constants cannot be definitely determined; but the result of solving these linear equations and substituting their values in S will be expressible in the form

$$\sum_{j=1}^{j=m} C_j S_j,$$

where C_j is an arbitrary constant and S_j is a substitutional expression containing no arbitrary constant, which is such that the result of substituting S_j for P in each of the substitutional equations is zero, in virtue of the multiplication table of the group. Every solution may then be written in the form

$$P=\sum_i\,[\sum_j C_{j,i}\,S_j]\,F_i\doteq\sum_j S_j\,[\sum_i C_{j,i}\,F_i]=\sum_j S_j\Phi_j,$$

where $C_{j,i}$ is a definite constant

$$\Phi_j=\sum_i C_{j,i}\,F_i,$$

and F_i and P are functions of the nature under discussion.

An expression in terms of which every solution can be expressed, such as $\Sigma_j S\ \Phi_j$, we call the complete solution of the system of equations. It will be seen later on that this is not always unique.

It is well to remark that it is not necessary to take S equal to the sum of all the substitutions of the symmetric group of the variables with arbitrary coefficients. It is sufficient that S should contain all the substitutions of the smallest group G which contains all those substitutions which actually occur in the expressions of our equations. For, if $G = 1+s_2+\ldots+s_\rho$, it is well known that it is possible to obtain a table

$$\begin{array}{lllll} 1, & s_2, & s_3, & \ldots, & s_\rho, \\ \sigma_2, & s_2\sigma_2, & s_3\sigma_2, & \ldots, & s_\rho\sigma_2, \\ \ldots & \ldots & \ldots & \ldots & \\ \sigma_{\rho'}, & s_2\sigma_{\rho'}, & s_3\sigma_{\rho'}, & \ldots, & s_\rho\sigma_{\rho'}, \end{array}$$

such that every substitution of the symmetric group is contained once, and only once, in the table; and, further, that the result of multiplying on the left-hand side any substitution in this table by one of the substitutions in G changes it to another substitution in the same horizontal line. Hence, if S be the sum of all the substitutions of the symmetric group with arbitrary coefficients, the substitutional equations only give relations between the constants in the same horizontal line, and the relations for the various lines are the same.

As an example, consider the equation

$$\{(\mathrm{abcd})\}\,P = 0$$

$$S = A_1+A_2\,(\mathrm{abcd})+A_3\,(\mathrm{ac})(\mathrm{bd})+A_4\,(\mathrm{adcb}).$$

Equating the coefficients in $\{(\mathrm{abcd})\}\,S$ to zero, we obtain

$$A_1+A_2+A_3+A_4 = 0.$$

Hence

$$\begin{aligned} S &= -A_2-A_3-A_4+A_2\,(\mathrm{abcd})+A_3\,(\mathrm{abcd})^2+A_4\,(\mathrm{abcd})^3 \\ &= \left[1-(\mathrm{abcd})\right]\left[-A_2-A_3\{1+(\mathrm{abcd})\}-A_4\{1+(\mathrm{abcd})+(\mathrm{abcd})^2\}\right]. \end{aligned}$$

And the complete solution is

$$[1-(\mathrm{abcd})]\,F.$$

3. Consider now a single equation, or a system of equations, of the form
$$[\lambda_1+\lambda_2 s_2+\lambda_3 s_3+\ldots]\,P = R,$$
where, as before, λ_1, λ_2, ... are constants, s_2, s_3, ... substitutions, and R

is a given rational integral algebraic function of the variables. It is, in the first place, to be noticed that the above equation in general implies a restriction on R, viz., that R can be written in the form $[\lambda_1+\lambda_2 s_2+\ldots]\,F$, and, as a consequence, satisfies certain substitutional equations. Thus, if $\lambda_1+\lambda_2 s_2+\ldots = G$ the sum of the substitutions of a group, R must belong to the group G. Let P_1 be any solution of the equations; then, if P_2 be another solution,

$$[\lambda_1+\lambda_2 s_2+\ldots]\,(P_1-P_2) = 0.$$

Hence, as in linear differential equations, the work of solution may be divided into two parts. First, any particular solution P_1 is found; and then—what corresponds to the complementary function—the complete solution Q of the system

$$[\lambda_1+\lambda_2 s_2+\ldots]\;Q = 0.$$

The complete solution—that is, the solution in terms of which every other can be expressed—is then

$$P = P_1+Q.$$

It will be seen later on, in the applications made to the quadratic and quartic invariants, that, in general, R is subject to more conditions than that implied by

$$R = [\lambda_1+\lambda_2 s_2+\ldots]\;F$$

when a simultaneous system of such equations is under discussion.

4. It may happen that the only solution of an equation

$$[\lambda_1+\lambda_2 s_2+\ldots]\;P = 0 \qquad \text{(I.)}$$

is $P=0$. Let G be the group of the substitutions which appear in this equation; then, if s be any substitution of G,

$$s\,[\lambda_1+\lambda_2 s_2+\ldots]\;P = 0.$$

Operating, then, on (I.) with each of the ρ substitutions of G, where ρ is the order of G, we obtain ρ linear equations with constant coefficients between the ρ quantities

$$P,\; s_2 P,\; \ldots$$

regarded as independent variables. The necessary and sufficient condition that there may be a solution other than zero is then expressed by the vanishing of a determinant of ρ columns and rows.

If $\quad \lambda_1+\lambda_2 s_2+\ldots = G = 1+s_2+s_3+\ldots+s_\rho,$

the sum of the substitutions of a group G of order ρ, the complete solution of (I.) is of the form

$$P = \Sigma \left(A_1 + A_2 s_2 + \ldots + A_\rho s_\rho\right) F,$$

where $$G\left(A_1 + A_2 s_2 + \ldots + A_\rho s_\rho\right) \equiv 0.$$

This gives $$A_1 + A_2 + \ldots + A_\rho = 0.$$

Hence

$$A_1 + A_2 s_2 + \ldots + A_\rho s_\rho = A_2\left(s_2 - 1\right) + A_3\left(s_3 - 1\right) + \ldots + A_\rho\left(s_\rho - 1\right).$$

Now, let $\sigma_1, \sigma_2, \ldots, \sigma_m$ be any substitutions of G which are not all contained in one of its sub-groups, and hence are sufficient to generate G. Then every substitution s of G can be expressed in the form

$$s = \sigma_{r_1}^{a_1} \sigma_{r_2}^{a_2} \ldots \sigma_{r_k}^{a_k},$$

where $r_1, r_2, \ldots, r_k$ are some of the numbers 1, 2, ..., m, not necessarily all different. But

$$s - 1 = \sigma_{r_1}^{a_1} s' - 1 = \left(\sigma_{r_1}^{a_1} - 1\right) s' + \left(s' - 1\right),$$

where $$s' = \sigma_{r_2}^{a_2} \ldots \sigma_{r_k}^{a_k},$$

and hence

$$\begin{aligned} s - 1 &= \left(\sigma_{r_1}^{a_1} - 1\right) \sigma_{r_2}^{a_2} \ldots \sigma_{r_k}^{a_k} + \left(\sigma_{r_2}^{a_2} - 1\right) \sigma_{r_3}^{a_3} \ldots \sigma_{r_k}^{a_k} + \ldots + \left(\sigma_{r_k}^{a_k} - 1\right) \\ &= \left(\sigma_1 - 1\right) S_1 + \left(\sigma_2 - 1\right) S_2 + \ldots + \left(\sigma_m - 1\right) S_m, \end{aligned}$$

where $S_1, S_2, \ldots, S_m$ are substitutional expressions, some of which may be zero, or merely numerical.

Hence

$$A_1 + A_2 s_2 + \ldots + A_\rho s_\rho = \left(\sigma_1 - 1\right) T_1 + \left(\sigma_2 - 1\right) T_2 + \ldots + \left(\sigma_m - 1\right) T_m,$$

where $T_1, T_2, \ldots, T_m$ are substitutional expressions containing the arbitrary constants $A_2, A_3, \ldots, A_\rho$.

Moreover $$G(\sigma - 1) = 0\,;$$

hence the complete solution of the equation

$$GP = 0$$

may be written

$$P = \left(\sigma_1 - 1\right) F_1 + \left(\sigma_2 - 1\right) F_2 \ldots + \left(\sigma_m - 1\right) F_m,$$

$F_1, F_2, \ldots, F_m$ being arbitrary functions.

Similarly, the complete solution of the equation

$$GP = R,$$

R necessarily belonging to the group G, is

$$P = \frac{R}{\rho} + (\sigma_1 - 1) F_1 + (\sigma_2 - 1) F_2 + \dots + (\sigma_m - 1) F_m,$$

for

$$\frac{1}{\rho} GR = R,$$

and consequently $\frac{R}{\rho}$ is a particular solution.

If, for instance, $G = \{a_1 a_2 \dots a_n\}$,

any one of the three following expressions may be taken as the complete solution :—

$$\{a_1 a_2\}' F_1 + \{a_1 a_3\}' F_2 + \dots + \{a_1 a_n\}' F_n,$$

$$\{a_1 a_2\}' F_1 + \{a_2 a_3\}' F_2 + \dots + \{a_{n-1} a_n\}' F_n,$$

$$\{a_1 a_2\}' F_1 + [1 - (a_1 a_2 a_3 \dots a_n)] F_2 :$$

an illustration of the remark already made, that it would be found that the complete solution was not always unique.

It follows from the above that the solution of

$$\{G_1, G_2\} P = 0$$

may be written

$$P = P_1 + P_2,$$

where

$$G_1 P_1 = 0 \quad \text{and} \quad G_2 P_2 = 0.$$

For we may choose substitutions $\sigma_1, \sigma_2, \dots, \sigma_h$ which generate G_1, and substitutions $\sigma_{h+1}, \sigma_{h+2}, \dots, \sigma_m$ which generate G_2; these substitutions will then together generate $\{G_1, G_2\}$. The solution of

$$\{G_1, G_2\} P = 0$$

may then be written

$$P = (\sigma_1 - 1) F_1 + \dots + (\sigma_h - 1) F_h + (\sigma_{h+1} - 1) F_{h+1} + \dots + (\sigma_m - 1) F_m$$

$$= P_1 + P_2,$$

where

$$P_1 = (\sigma_1 - 1) F_1 + \dots + (\sigma_h - 1) F_h$$

and

$$P_2 = (\sigma_{h+1} - 1) F_{h+1} + \dots + (\sigma_m - 1) F_m,$$

and consequently $G_1 P_1 = 0$ and $G_2 P_2 = 0$.

5. When all the substitutions are powers of a single substitution the equations are easy to solve. Consider a single equation, the most general of its kind,

$$\phi(s)\,P = (A_0 + A_1 s + A_2 s^2 + \ldots + A_{n-1} s^{n-1})\,P = 0,$$

where s is a substitution of order n.

We require to find the most general expression

$$\psi(s) = (B_0 + B_1 s + B_2 s^2 + \ldots + B_{n-1} s^{n-1}),$$

which is such that $\phi(s)\,\psi(s) \equiv 0.$

Now $\phi(x)\,\psi(x)$ only vanishes when $\phi(x) = 0$, or when $\psi(x) = 0$. Neither of these cases need be discussed here; then the product $\phi(s)\,\psi(s)$ must vanish solely in consequence of the equation

$$s^n = 1.$$

Hence $\phi(x)\,\psi(x) = (x^n - 1)\,\chi(x).$

To find ψ, we then obtain the H.C.F. of $x^n - 1$ and $\phi(x)$, say $\phi_1(x)$; then

$$\psi(x) = \frac{x^n - 1}{\phi_1(x)}.$$

Now, if a is not a root of $x^n - 1 = 0$,

any function Q may be written in the form

$$Q = (s^{n-1} + a s^{n-2} + \ldots + a^{n-1})\,F = \left[\frac{s^n - a^n}{s - a}\right] F = \left[\frac{1 - a^n}{s - a}\right] F,$$

for $Q = \frac{s^n - a_n}{1 - a^n}\,Q = (s^{n-1} + a s^{n-2} + \ldots + a^{n-1})\left(\frac{s - a}{1 - a^n}\,Q\right).$

Hence, if $\phi(x) = \phi_1(x)(x - a_1)(x - a_2)\ldots(x - a_r),$

any solution P of the equation may be written

$$\begin{aligned} P = \psi(s)\,F &= \left[\frac{s^n - 1}{\phi_1(s)}\right] F \\ &= \left[\frac{s^n - 1}{\phi_1(s)}\right]\left[\frac{1}{(s - a_1)(s - a_2)\ldots(s - a_r)}\right] E \\ &= \left[\frac{s^n - 1}{\phi(s)}\right] E, \end{aligned}$$

where it is to be understood that the expression $\frac{1}{s - a_1}$ is equivalent to $\frac{s^{n-1} + a s^{n-2} + \ldots + a^{n-1}}{1 - a_1^n}$, when a_1^n is not equal to unity.

It has been tacitly assumed that $\phi(s)$ has no squared factor which is also a factor of s^n-1; if such should occur, we may remove it by adding to $\varphi(s)$ a multiple of s^n-1, which is in actual value zero, and then proceed as before. If $\phi(s)$ has no common factor with s^n-1, then $P=0$.

To find a particular solution of

$$\phi(s)\,P = R.$$

The restriction imposed on R by this equation is

$$\frac{s^n-1}{\varphi_1(s)}\,R = 0.$$

Hence $$R = \varphi_1(s)\,R'.$$

If there is no difficulty in finding R' from this, the particular solution

$$P = \frac{\phi_1(s)}{\varphi(s)}\,R'$$

may be taken.

If the form of R' is not at once obvious, the particular solution may be found thus:—

$$\phi_1(s)\,\phi_1(s) = \varphi_1(s)\,\varphi_1(s) + \lambda\,(s^n-1) = \phi_1(s)\,\psi_2(s),$$

where s^n-1 and $\phi_2(s)$ have no common factor. Then

$$\varphi_1(s)\,\phi(s)\,P = \varphi_1(s)\,R = \phi_1(s)\left[\frac{\Phi(s)}{\varphi_1(s)}\,\phi_2(s)\right]P,$$

and $$\left[\frac{\phi_1(s)}{\varphi(s)\,\varphi_2(s)}\right]R$$

is a solution.

The extension to any set of simultaneous equations involving only powers of s is obvious.

Also it may be seen, in the same way, that the solution of any set of Abelian equations is a matter only of algebra.

Single equations which are not merely formed by the sum of the substitutions of a group, and in which the substitutions are not all contained in an Abelian group, may frequently be solved with the help of the solutions in these two cases. Thus, the solution of the equation $$\{\mathrm{ab}\}\,[1+(\mathrm{abcd})+(\mathrm{abcd})^2]\,P = R$$

—which occurs in the reduction of the quartic invariant types—is

$$P = \tfrac{1}{3}\,[1-2\,(\mathrm{abcd})+(\mathrm{abcd})^2+(\mathrm{abcd})^3]\left[\frac{R}{2}+\{\mathrm{ab}\}'\,F\right],$$

and R must satisfy the equation

$$\{ab\}' R = 0.$$

6. Consider now two simultaneous equations

$$\{s\}\, P = 0, \quad \{\sigma\}\, P = 0.$$

Then, if

$$s\sigma \equiv \tau_1, \quad \sigma s \equiv \tau_2,$$

$$\sigma\tau_1^n = \tau_2^n\sigma, \quad \tau_1^n = s\tau_2^{n-1}\sigma.$$

Hence, if m be the order of τ_1,

$$\tau_2^m = \sigma\tau_1^m\sigma^{-1} = 1,$$

and the orders of τ_1 and τ_2 must be identical.

Also the expression $(1-\sigma)\{\tau_1\} = (s-1)\{\tau_2\}\,\sigma.$

Hence

$$P = (1-\sigma)\,\{\tau_1\}\,F$$

is a solution of the equations.

Unfortunately this is not always the complete solution, for suppose that

$$s\sigma = \sigma s, \quad s^2 = 1, \quad \sigma^3 = 1\,;$$

then the complete solution may be written

$$P = (1-s)(1-\sigma)\,F;$$

but the expression $(1-\sigma)\{\tau_1\}$ vanishes identically, for $\{\tau_1\}$ is here equal to $\{s, \sigma\}$.

Again, whenever the substitutions s, σ are permutable, the solution

$$P = (1-\sigma)\,\{\tau_1\}\,F,$$

in addition to satisfying the two equations

$$\{s\}P = 0, \quad \{\sigma\}\,P = 0,$$

belongs to the group $\{\tau_1\}$, which is not in general the case with the complete solution

$$P = (1-\sigma)(1-s)\,F.$$

However, whenever

$$s^2 = 1 = \sigma^2,$$

the complete solution may be written

$$P = (1-\sigma)\,\{\tau_1\}\,F,$$

for

$$\{s, \sigma\} = \{\sigma, \tau_1\} = \{\sigma\}\,\{\tau_1\},$$

since

$$\tau_1\sigma = s = \sigma\tau_1^{-1}.$$

Hence we may write $S = \Sigma\,(1+A_a\sigma)\,B_a\tau_1^a$.

and find S, so that $\{s\}\,S=0$ and $\{\sigma\}\,S=0$.

The second equation gives $A_a=-1$.

$$\text{Hence}\quad S=(1-\sigma)(B_0+B_1\tau_1+\ldots+B_{m-1}\tau_1^{m-1})$$

$$=\left[s\,(B_0\tau_2^{m-1}+B_1+B_2\tau_2+\ldots+B_{m-1}\tau_2^{m-2})\right.$$

$$\left.-(B_0+B_1\tau_2+\ldots+B_{m-1}\tau_2^{m-1})\right]\sigma.$$

The equation $\{s\}\,S=0$

then gives $B_0=B_1=\ldots=B_{m-1}$.

Hence the complete solution is as stated.

A solution of any number of equations

$$\{s_1\}\,P=0,\ \{s_2\}\,P=0,\ \ldots,\ \{s_n\}\,P=0$$

may then be seen to be

$$P=(1-s_1)\,\{s_2s_1,\ s_3s_1,\ \ldots,\ s_ns_1\}\,F.$$

If each of the substitutions $s_1, s_2, \ldots, s_n$ is of order 2, this is the complete solution. For it can be written in the form

$$P=(1-s_1)\,E,$$

where E is a rational integral algebraic function of the variables, since

$$\{s_1\}\,P=0;$$

and by what we have seen above E must belong to the group $\{s_2s_1\}$, if

$$\{s_2\}\,P=0.$$

Hence E must belong to the smallest group containing $s_2s_1, s_3s_1, \ldots, s_ns_1$.

7. It frequently happens that a function is given as belonging to a certain group, besides satisfying certain substitutional equations. Thus, the invariant type degree 5 of a quartic belongs to the group $\{(\text{abcde}), (\text{ae})(\text{bd})\}$, and satisfies the equation

$$\{\text{abc}\}\,I_5=R,$$

the other equations which it satisfies being consequences of these facts. Further, in the case of irreducible invariants, we really only require to find the number of invariants of the form I_5 in terms of which the rest can be linearly expressed. In respect to this, we shall prove that:

If M be the number of arbitrary constants in the most general substitutional expression S_1, which may contain all the $n!$ substitutions of the symmetric group of the n variables under consideration, which satisfies the equations

$$G_1 S_1 \equiv 0, \quad G_2 S_1 \equiv r_2 S_1,$$

G_1 and G_2 being groups of orders r_1 and r_2 respectively, and if N be the number of arbitrary constants in the most general substitutional expression S_2 which satisfies the equations

$$G_2 S_2 \equiv 0, \quad G_1 S_2 \equiv r_1 S_2,$$

then

$$M - N = n! \left\{ \frac{1}{r_2} - \frac{1}{r_1} \right\}.$$

Consider S_1, and suppose that at first all the coefficients are arbitrary. Let A_s be the coefficient of s; then the equation

$$G_1 S_1 \equiv 0$$

gives $\frac{n!}{r_1}$ equations of the form

$$\Sigma A_s = 0, \tag{I.}$$

and in no two of these equations does the same coefficient occur. Now, if σ be any substitution of G_2, it follows that, since S_1 has G_2 for a factor,

$$A_{\sigma s} = A_s.$$

Owing to this, there are only $\frac{n!}{r_2}$ different coefficients; and, if this be taken into account, the equations (I.) are not all independent. Let $T = 0$ be any relation between these equations written out in full; then this is an identity solely on account of the equations $A_{\sigma s} = A_s$. Hence, if substitutions applied to T be supposed to operate on the suffixes of the A's, we have the equation

$$G_2 T = 0.$$

And, further, from the form of equations (I.),

$$G_1 T = r_1 T,$$

for $T = 0$ is a relation between different equations (I.). If, then, T'

be what T becomes when for each A_s we write s, T' will satisfy the equations for S_2. Hence, for every relation between the $\frac{n!}{r_1}$ equations to determine the $\frac{n!}{r_2}$ unknown constants in S_1, there is an expression of exactly the same form which satisfies the equations for S_2. Conversely, every solution of the equations for S_2 will give such a relation between the equations for the unknown constants in S_1. Hence the number of independent relations between the equations (I.) is N; consequently, the number of arbitrary constants left in S_1 when all the equations are satisfied is

$$M = \frac{n!}{r_2} - \left(\frac{n!}{r_1} - N\right);$$

and therefore $$M - N = n!\left(\frac{1}{r_2} - \frac{1}{r_1}\right).$$

Further, the number of those functions obtained from P by permuting the n variables, in terms of which the $n!$ possible functions thus obtained from P may be linearly expressed when P belongs to the group G_2 and satisfies

$$G_1 P = 0,$$

is equal to M, the number of arbitrary constants in the most general substitutional expression S_1 for which

$$G_1 S_1 \equiv 0, \quad G_2 S_1 \equiv r_2 S_1.$$

For, if P_s be the function obtained from P by operating on it with the substitution s, exactly the same linear equations exist between the functions P_s as between the coefficients A_s in S_1. Hence the number of linearly independent functions P_s is the same as the number of arbitrary coefficients in S_1.

8. If a function P satisfy each of the equations

$$\{a_1 a_2\} P = 0, \quad \{a_1 a_3\} P = 0, \quad \ldots, \quad \{a_1 a_n\} P = 0,$$

it is merely changed in sign when operated upon by any transposition of the letters $a_1, a_2, \ldots, a_n$. The complete solution of these equations is then

$$P = \{a_1 a_2 \ldots a_n\}' F.$$

The function P is an alternating function, and may be written, as is well known,

$$P = \sqrt{\Delta}\,\{\mathrm{a}_1\mathrm{a}_2\dots\mathrm{a}_n\}\,F',$$

where Δ is the product of the squares of the differences of the letters $a_1, a_2, \dots, a_n$.

Hence, if P is of degree less than $n-1$ in any one letter, it must be zero. Hence also, if Q be any rational integral function of degree $< n-1$ in each of its variables $a_2, a_2, \dots, a_n$, it satisfies the equation

$$\{\mathrm{a}_1\mathrm{a}_2\dots\mathrm{a}_n\}'\,Q = 0.$$

In this connection should be mentioned the following propositions already given for the quartic in my paper "On the Invariant Syzygies of Lowest Degree for any Number of Binary Quartics," viz.,

If P be a rational integral function homogeneous and linear in the coefficients of m binary n-ics,

$$(A_0^{(1)}, A_2^{(1)}, \dots, A_n^{(1)} \mathrel{)\!(} x_1, x_2)^n \dots (A_0^{(m)}, A_1^{(m)}, \dots, A_n^{(m)} \mathrel{)\!(} x_1, x_2)^n,$$

m being greater than $n+1$, then

$$\{\mathrm{A}^{(1)}\mathrm{A}^{(2)}\dots\mathrm{A}^{(n+2)}\}'\,P = 0, \qquad \text{(i.)}$$

$$\{\mathrm{A}^{(1)}\mathrm{A}^{(2)}\dots\mathrm{A}^{(n+1)}\}'P = |\,A^{(1)}A^{(2)}\dots A^{(n+1)}\,|\,P_1, \qquad \text{(ii.)}$$

$$\{\mathrm{A}^{(1)}\mathrm{A}^{(2)}\dots\mathrm{A}^{(n)}\}'P = |\,A^{(1)}A^{(2)}\dots A^{(n)}Q\,|\,, \qquad \text{(iii.)}$$

where a substitution $(\mathrm{A}^{(\alpha)}\mathrm{A}^{(\beta)})$ operating on P is regarded as interchanging (α) and (β) in all the indices in P; in fact it interchanges the positions held by the coefficients of the two quantics

$$(A_0^{(\alpha)}, A_1^{(\alpha)}, \dots, A_n^{(\alpha)} \mathrel{)\!(} x_1, x_2)^n, \quad (A_0^{(\beta)}, A_1^{(\beta)}, \dots, A_n^{\beta} \mathrel{)\!(} x_1, x_2)^n$$

in P; or else it may be regarded as an abbreviation for

$$(\mathrm{A}_0^{(\alpha)}\mathrm{A}_0^{(\beta)})(\mathrm{A}_1^{(\alpha)}\mathrm{A}_1^{(\beta)})\dots(\mathrm{A}_n^{(\alpha)}\mathrm{A}_n^{(\beta)}).$$

And $|\,A^{(1)}A^{(2)}\dots A^{(n+1)}\,|$ is the determinant of $n+1$ rows and columns formed by the coefficients of the $n+1$ quantics concerned; $|\,A^{(1)}A^{(2)}\dots A^{(n)}Q\,|$ is the same determinant with functions $Q_0, Q_1, \dots, Q_n$ of the coefficients of the quantics represented by $A^{(n+1)}, A^{(n+2)}, \dots, A^{(m)}$ of the same character as P, substituted for the coefficients $A_0^{(n+1)}$, $A_1^{(n+1)}, \dots, A_n^{(n+1)}$; and P_1 is a function, having the same character as

P, of the coefficients of the quantics represented by $A^{(n+2)} \dots A^{(m)}$. To prove (i.) we observe that P may be written in the form

$$P = \Sigma A^{(1)}_{r_1} A^{(2)}_{r_2} \dots A^{(n+2)}_{r_{n+2}} P',$$

where each of the suffixes $r_1, r_2, \dots, r_{n+2}$ is one of the $n+1$ numbers $0, 1, 2, \dots, n$; hence in any case two suffixes must be equal, and consequently

$$\{\mathbf{A}^{(1)}\mathbf{A}^{(2)} \dots \mathbf{A}^{(n+2)}\}' P = 0.$$

For (ii.) we write $$P = \Sigma A^{(1)}_{r_1} A^{(2)}_{r_2} \dots A^{(n+1)}_{r_{n+1}} P',$$

and here it is possible for the suffixes to be all different; if this is so,

$$\begin{aligned} \{\mathbf{A}^{(1)}\mathbf{A}^{(2)} \dots \mathbf{A}^{(n+1)}\}' A^{(1)}_{r_1} A^{(2)}_{r_2} \dots A^{(n+1)}_{r_{n+1}} &= \pm \{\mathbf{A}^{(1)}\mathbf{A}^{(2)} \dots \mathbf{A}^{(n+1)}\}' A^{(1)}_{0} A^{(2)}_{1} \dots A^{(n+1)}_{n+1} \\ &= \pm \mid A^{(1)} A^{(2)} \dots A^{(n+1)} \mid; \end{aligned}$$

and therefore

$$\{\mathbf{A}^{(1)}\mathbf{A}^{(2)} \dots \mathbf{A}^{(n+1)}\}' P = \mid A^{(1)} A^{(2)} \dots A^{(n+1)} \mid P_1.$$

As regards (iii.) we write

$$P = \Sigma A^{(1)}_{r_1} A^{(2)}_{r_2} \dots A^{(n)}_{r_n} P,$$

and distinguish the following cases :—first, terms R' in which two of the suffixes are equal; then terms R_0 in which the suffixes $r_1, r_2, \dots, r_n$ are the numbers $1, 2, \dots, n$ in some order; then terms R_1 in which the suffixes are the numbers $0, 2, 3, \dots, n$ in some order, and so on; finally, terms R_n in which the suffixes are $0, 1, 2, \dots, n-1$ in some order. Now operate with $\{\mathbf{A}^{(1)}\mathbf{A}^{(2)} \dots \mathbf{A}^{(n)}\}'$; then

$$\{\mathbf{A}^{(1)}\mathbf{A}^{(2)} \dots \mathbf{A}^{(n)}\}' R' = 0,$$

$$\{\mathbf{A}^{(1)}\mathbf{A}^{(2)} \dots \mathbf{A}^{(n)}\}' R_0 = \begin{vmatrix} A^{(1)}_1 A^{(1)}_2 \dots A^{(1)}_n \\ A^{(2)}_1 A^{(2)}_2 \dots A^{(2)}_n \\ \dots \quad \dots \quad \dots \\ A^{(n)}_1 A^{(n)}_2 \dots A^{(n)}_n \end{vmatrix} Q_0.$$

The other terms are found in the same way; so that, taking the sum,

$$\{\mathbf{A}^{(1)}\mathbf{A}^{(2)} \dots \mathbf{A}^{(n)}\}' P = \mid A^{(1)} A^{(2)} \dots A^{(n)} Q \mid.$$

9. As an example, consider the invariants of any number of binary quadratics

$$a_x^2,\ b_x^2,\ \dots .$$

The possible invariant forms are

$$(ab)^2,\ (ab)(bc)(ca),\ (ab)(bc)(cd)(da),\ \dots;$$

then $\{\mathrm{bc}\}(ab)(bc)(cd) = (ab)(bc)(cd)-(ac)(bc)(bd) = -(bc)^2(ad)$;

so that, if b, c be any pair of consecutive letters in an invariant I, $\{\mathrm{bc}\}\,I$ is reducible.

Again,

$$\begin{aligned}\{\mathrm{bd}\}'(ab)(bc)(cd)(de) &= (ab)(bc)(cd)(de)-(ad)(dc)(cb)(be)\\ &= (bc)(cd)(db)(ae).\end{aligned}$$

Similarly, any other interchange of letters may be dealt with. The number of irreducible invariants I of any degree n is equal to the number of linearly independent functions obtained from the function P by permuting the letters which it contains, when P satisfies the equations

$$\{\mathrm{ab}\}\,P = 0,\ \{\mathrm{bc}\}\,P = 0,\ \dots,\ \{\mathrm{ac}\}'\,P = 0,\ \dots,$$

and, in fact, all the equations which I satisfies, with the right-hand side of each replaced by zero [I being supposed $= (ab)(bc)(cd)\dots(ha)$].

If n, the degree of I, be greater than 3, then by the last article

$$\{\mathrm{abcd}\}'\,I = 0.$$

Since $\{\mathrm{ab}\}\,P = 0,\ \{\mathrm{bc}\}\,P = 0,\ \dots,\ \{\mathrm{ha}\}\,P = 0,$

$$P = \{\mathrm{abc}\dots\mathrm{h}\}'\,F = \frac{1}{n!}\{\mathrm{abc}\dots\mathrm{h}\}'\,P = 0,$$

and I is reducible when $n > 3$. If the actual solution of the equations for I be carried out, it will be found that in general the expressions on the right-hand side have to satisfy relations; these relations will be the syzygies degree n for the quadratic invariant types. In regard to these equations, it should be noticed that in each separate equation for quadratic types, of the form

$$[\lambda_1+\lambda_2 s_2+\lambda_3 s_3+\dots]\,I = R,$$

where R is a given reducible expression, it is obviously true that R possesses the substitutional properties involved in the operator on the left. The syzygies arise from the fact that I satisfies more than e equation of this kind. Hence R is subject, owing to the system equations, to more conditions than those implied by the operator the left-hand side. Exactly the same remark applies to the uations for quartic invariant types of degree greater than 6. he equations in their complete form for degree 7 are given in my per, "On the Invariant Syzygies of Lowest Degree for any umber of Binary Quartics," already quoted.

As has been pointed out at the commencement of this paper, the variants of any number of quartics give another illustration of substitutional equations. Thus, the invariant type (*abcde*), degree 5, tisfies the equation

$$\{\mathrm{abc}\}\,(abcde) = R,$$

d is of group $\{(\mathrm{abcde}),\ (\mathrm{be})(\mathrm{cd})\}$. It has been shown that there e only six independent irreducible forms (*abcde*). If, now, the eorem of § 7 be applied, we find that, if M be the number of the nctions obtained from $[abcde]$ by interchanging the variables in rms of which all the functions obtained by every possible interange can be linearly expressed, where $[abcde]$ is defined as being group $\{\mathrm{abc}\}$ and as satisfying the equation

$$\{(\mathrm{abcde}),\ (\mathrm{be})(\mathrm{cd})\}\,[abcde] = 0$$

en $$M-6 = 5!\,(\tfrac{1}{6}-\tfrac{1}{10}) = 8$$

d $$M = 14.$$

10. In what follows repeated use will be made of the symmetric oup; it is convenient, then, to note that the sum of its substitutions ay be factorized in a variety of ways. For instance,

$$\begin{aligned}\{\mathrm{a}_1\mathrm{a}_2\ldots\mathrm{a}_n\} &= \{(\mathrm{a}_1\mathrm{a}_2\ldots\mathrm{a}_n)\}\,\{\mathrm{a}_1\mathrm{a}_2\ldots\mathrm{a}_{n-1}\}\\ &= \left[1+(\mathrm{a}_1\mathrm{a}_n)+(\mathrm{a}_2\mathrm{a}_n)+\ldots+(\mathrm{a}_{n-1}\mathrm{a}_n)\right]\{\mathrm{a}_1\mathrm{a}_2\ldots\mathrm{a}_{n-1}\}\\ &= \{\mathrm{a}_1\mathrm{a}_2\}\,G_n,\end{aligned}$$

here G_n is the alternating group of the n letters.

Now, any purely formal relation between functions of substitutions ill still hold good if the sign of every transposition be changed, ence the negative symmetric group may be factorized in the same ay, thus

$$\{\mathrm{a}_1\mathrm{a}_2\ldots\mathrm{a}_n\}' = \left[1-(\mathrm{a}_1\mathrm{a}_n)-(\mathrm{a}_2\mathrm{a}_n)-\ldots-(\mathrm{a}_{n-1}\mathrm{a}_n)\right]\{\mathrm{a}_1\mathrm{a}_n\ldots\mathrm{a}_{n-1}\}'.$$

Again, the product of a group by itself is the group multiplied by a constant factor equal to its order. The product of a group by a sub-group is equal to the whole group multiplied by the order of the sub-group; for, if G be the whole group, and S a substitution belonging to the sub-group G_1, then

$$G.s = G.$$

Again, if $\{a_1 a_2 a_3 \dots a_n\}$ be any positive symmetric group, and $\{a_1 a_2 b_3 \dots b_m\}'$ a negative symmetric group,

$$\begin{aligned} & \{a_1 a_2 a_3 \dots a_n\} \{a_1 a_2 b_3 \dots b_m\}' \\ = \quad & \{a_1 a_2 a_3 \dots a_n\} (a_1 a_2) \left[-(a_1 a_2) \{a_1 a_2 b_3 \dots b_m\}' \right] \\ = & - \{a_1 a_2 a_3 \dots a_n\} \{a_1 a_2 b_3 \dots b_m\}' = 0. \end{aligned}$$

Let $S[a_1 b_1 b_2 \dots b_m]$ be any substitutional expression affecting the letters $a_1, b_1, b_2, \dots, b_m$, and only these; then

$$\{a_2 a_3 \dots a_n\} S[a_1 b_1 b_2 \dots b_m] = S[a_1 b_1 b_2 \dots b_m] \{a_2 a_3 \dots a_n\}.$$

Hence $\qquad \{a_1 a_2 \dots a_n\} S[a_1 b_1 b_2 \dots b_m] \{a_1 a_2 \dots a_n\}$

$$\begin{aligned} &= [1+(a_1 a_2)+(a_1 a_3)+\dots+(a_1 a_n)] \{a_2 a_3 \dots a_n\} S[a_1 b_1 b_2 \dots b_m\} \\ &\qquad\qquad \times \{a_1 a_2 \dots a_n\} \\ &= (n-1)! \, [1+(a_1 a_2)+(a_1 a_3)+\dots+(a_1 a_n)] S[a_1 b_1 b_2 \dots b_m] \{a_1 a_2 \dots a_n\} \\ &= (n-1)! \left[S[a_1 b_1 b_2 \dots b_m] + S[a_2 b_1 b_2 \dots b_m] + \dots + S[a_n b_1 \dots b_m] \right] \\ &\qquad\qquad \times \{a_1 a_2 \dots a_n\}; \end{aligned}$$

or, as may be proved in the same way,

$$\begin{aligned} &= (n-1)! \{a_1 a_2 \dots a_n\} \left[S[a_1 b_1 \dots b_m] + S[a_2 b_1 \dots b_m] + \dots \right. \\ &\qquad\qquad \left. \dots + S[a_n b_1 \dots b_m] \right]. \end{aligned}$$

11. As certain results, due in the first place to Capelli, are to be obtained in this paper by means of substitutional analysis, some account of the remarkable paper, "Sur les Opérations dans la Théorie des Formes Algébriques,"[*] in which they occur, is given here. In this paper Capelli considers functions rational, integral, algebraic,

---

[*] *Math. Ann.*, Bd. XXXVII., pp. 1-37.

of n sets of variables

$$\begin{array}{cccc} x_1, & x_2, & \dots, & x_m, \\ y_1, & y_2, & \dots, & y_m, \\ \dots & & \dots & \dots \\ u_1, & u_2, & \dots, & u_m, \end{array}$$

there being m variables in each set, and homogeneous in the variables of each set. Such a function is written

$$f(x, y, \dots, u).$$

He regards the polar operation

$$D_{xy} = y_1 \frac{\partial}{\partial x_1} + y_2 \frac{\partial}{\partial x_2} + \dots + y_m \frac{\partial}{\partial x_m}$$

as fundamental, and proceeds in the first section to develop a theory of operations which can be expressed as rational integral functions with constant coefficients of operations of this kind, and proves that, if by Δ be understood some operation which can be thus expressed, every function $f(x, y, \dots, u)$ of the above sets of variables which is homogeneous and of degree a_i in the variables whose index is i, for all values of i from 1 up to m, can be obtained in the form

$$f(x, y, \dots, u) = \Delta x_1^{a_1} y_2^{a_2} \dots v_m^{a_m},$$

there being the same number of sets expressed in the term on which Δ operates as there are variables in each set, Δ depending on the form of f.

His second section is devoted to the discussion of an operation H defined as follows :—

$$\text{If } m = n, \quad H = |\, xy \dots u \,| \left| \frac{\partial}{\partial x} \frac{\partial}{\partial y} \dots \frac{\partial}{\partial u} \right|,$$

$$\text{if } m > n, \quad H = \sum_i |\, x_{i_1} y_{i_2} \dots u_{i_n} \,| \left| \frac{\partial}{dx_{i_1}} \frac{\partial}{\partial x_{i_2}} \dots \frac{\partial}{\partial u_{i_n}} \right|,$$

$$\text{is } m < n, \quad H = 0,$$

where $|\, xy \dots u \,|$ is the determinant formed by the variables, and $\left| \frac{\partial}{\partial x} \frac{\partial}{\partial y} \dots \frac{\partial}{\partial u} \right|$, which is the determinant formed by the first differential operators with respect to the variables, is Cayley's operator Ω.

It is shown that H may be expressed in terms of the operators

D_{xy}, and the form of this expression is found; further, it is proved that H is commutative with all rational integral functions of the operators D_{xy}. It is then proved that, if a function $f(x, y, z, \ldots, t, u)$ of the kind considered, of n sets of variables, there being n variables in each set, is annihilated by each of D_{xy}, D_{yz}, ..., D_{tu}, it is equal to a power of $| xyz \ldots tu |$ multiplied by a function of the same nature of the sets $y, z, \ldots, t, u$, which is annihilated by $D_{yz}, \ldots, D_{tu}$.

In the third section it is proved that, if two functions of the same number of sets of variables, rational, integral, and homogeneous in the variables of each set, are obtainable from each other by means of a permutation of the sets, they are also obtainable from each other by means of the operators D_{xy}. In other words, an operator which is a rational, integral function of the operators D_{xy} may be always found which will have the same effect on $f(x, y, \ldots, u)$ as any given substitution operating on this function. In view of the importance of this theorem in connection with the present subject, I quote Capelli's illustration. Let $f(x, y, z)$ be any rational, integral function of the variables

$$\begin{matrix} x_1, & x_2, & \ldots, & x_m, \\ y_1, & y_2, & \ldots, & y_m, \\ z_1, & z_2, & \ldots, & z_m, \end{matrix}$$

homogeneous and of degrees λ, μ, ν respectively in the variables of the three sets. Let

$$\begin{matrix} \xi_1, & \xi_2, & \ldots, & \xi_m, \\ \eta_1, & \eta_2, & \ldots, & \eta_m, \\ \zeta_1, & \zeta_2, & \ldots, & \zeta_m \end{matrix}$$

be three new sets of variables, independent of each other and of the original sets; then

$$f(\xi, \eta, \zeta) = \frac{1}{\lambda!\,\mu!\,\nu!} D^{\lambda}_{x\xi} D^{\mu}_{y\eta} D^{\nu}_{z\zeta} f(x, y, z),$$

and $$f(y, z, x) = \frac{1}{\lambda!\,\mu!\,\nu!} D^{\lambda}_{\xi y} D^{\mu}_{\eta z} D^{\nu}_{\zeta x} f(\xi, \eta, \zeta);$$

hence $$f(y, z, x) = \left(\frac{1}{\lambda!\,\mu!\,\nu!}\right)^2 D^{\lambda}_{\xi y} D^{\mu}_{\eta z} D^{\nu}_{\zeta x} D^{\lambda}_{x\xi} D^{\mu}_{y\eta} D^{\nu}_{z\zeta} f(x, y, z).$$

By means of the methods laid down in the first section of Capelli's paper, it is possible to reduce this to the form $\Delta f(x, y, z)$, where the operators of which Δ is a function only affect the sets x, y, z.

In this section it is also proved that the condition that f should be expressible as a sum of terms each of which is derivable by operations of the kind considered from functions of a smaller number of sets of variables than that contained in f is

$$H.f = 0.$$

In § 4 the following important theorem is proved:

If $f(x, y, \dots, u)$ is a rational, integral function of n sets of variables, there being n variables in each set, which is homogeneous in the variables of each set, then

$$f(x, y, \dots, u) = \sum_{\mu, i} | xy \dots u |^{\mu} . \Delta_i . \phi_i (y, z, \dots, u),$$

where $\phi_i (y, z, \dots, u) = D_{xy}^{\alpha_i} D_{xz}^{\beta_i} \dots D_{xu}^{\lambda_i} . \Omega^{\mu} f$;

the Σ extending to all positive integral solutions of

$$\alpha_i + \beta_i + \dots + \lambda_i + \mu = p,$$

where p is the degree of f in x, and where Δ_i is a rational integral function with constant coefficients of operators of the form D_{xy}, the form of which depends only on the degrees in which the variables occur in f; and, further, the coefficients of different powers of $| xy \dots u |$ are unique. The last section is devoted to an extension of certain of the results to any analytic function.

12. In what follows substitutions are taken as the fundamental operators, instead of Capelli's operators D_{xy}. Functions $f(a, b, \dots, k)$ are considered which are rational, integral, homogeneous, and linear in each of n sets of variables

$$a_1, a_2, \dots, a_m,$$
$$b_1, b_2, \dots, b_m,$$
$$\dots \quad \dots \quad \dots$$
$$k_1, k_2, \dots, k_m,$$

[illegible] being m variables in each set. The letters $a, b, \dots, k$ are [illegible] as the applications considered are mainly to concomitant [illegible] of quantics. The restriction that f is to be linear in the [illegible] of each set does not in reality restrict the generality of the [illegible] [illegible]; for, if $F(a, b, \dots, k)$ be a function rational, integral, homogeneous, and of degrees $\alpha, \beta, \ldots, \kappa$ in the variables of the different sets, we may obtain a function f, such that

$$f(a^{(1)}, a^{(2)}, \ldots, a^{(\alpha)}, b^{(1)}, \ldots, b^{(\beta)}, \ldots, k^{(\kappa)})$$

$$= \frac{1}{\alpha!\,\beta!\ldots\kappa!} D_{aa^{(1)}} D_{aa^{(2)}} \ldots D_{aa^{(\alpha)}} D_{bb^{(1)}} \ldots D_{kk^{(\kappa)}} F(a, b, \ldots, k),$$

and consider, instead of F, the function

$$\frac{1}{\alpha!\,\beta!\ldots\kappa!} \{\mathrm{a}^{(1)}\mathrm{a}^{(2)} \ldots \mathrm{a}^{(\alpha)}\} \{\mathrm{b}^{(1)} \ldots \mathrm{b}^{(\beta)}\} \ldots \{\mathrm{k}^{(1)} \ldots \mathrm{k}^{(\kappa)}\} f,$$

For, if we write

$$a^{(1)} = a^{(2)} = \ldots = a, \quad b^{(1)} = \ldots = b, \quad \ldots, \quad k^{(1)} = \ldots = k,$$

this becomes F once more. There is a fairly close connexion between the theory of substitutional and of polar operators. Thus any function $f(a, b, \ldots, k)$ of n sets of variables, there being m variables in each set, which is homogeneous and linear in the variables of each set, and homogeneous and of degree α_i in the variables whose index is i, for all values of i from 1 up to m, may be expressed in the form

$$f(a, b, \ldots, k) = S a_1^{(1)} \ldots a_1^{(\alpha_1)} b_2^{(1)} \ldots b_2^{(\alpha_2)} \ldots k_m^{(\alpha_m)},$$

where S is a substitutional operator with constant coefficients. This follows at once from § 1; for there is only one kind of term which can occur here.

The operator H may be expressed as a substitutional operator thus:—We first suppose that H is to operate on a function homogeneous and linear in the variables of each of n sets, there being n variables in each set; then

$$H = | ab \ldots k | \left| \frac{\partial}{\partial a} \frac{\partial}{\partial b} \cdots \frac{\partial}{\partial k} \right|.$$

But in this case

$$| ab \ldots k | \left| \frac{\partial}{\partial a} \frac{\partial}{\partial b} \cdots \frac{\partial}{\partial k} \right| f = \{\mathrm{ab} \ldots \mathrm{k}\}' f.$$

For, if $A a_{i_1} b_{i_2} \ldots k_{i_m}$ be any term of f, the effect of both operators is zero, unless all the indices are different, and, if this is so, both operators give $A \mid ab \ldots k \mid$ as the result, the rule for determining the sign being the same in each case.

If f is still linear in the variables of each set, but the number of variables in a set is m, greater than the number n of sets, then H is still equivalent to $\{\mathrm{ab} \dots \mathrm{k}\}'$, for, if $Aa_{i_1} b_{i_2} \dots k_{i_m}$ be any term of f, then

$$\{\mathrm{ab} \dots \mathrm{k}\}\, A a_{i_1} b_{i_2} \dots k_{i_m}$$

$$= \left| a_{i_1} b_{i_2} \dots k_{i_m} \right| \left| \frac{\partial}{\partial a_{i_1}} \frac{\partial}{\partial b_{i_2}} \cdots \frac{\partial}{\partial k_{i_m}} \right| A a_{i_2} \dots k_{i_m}$$

$$= \left[\sum_j \left| a_{j_1} b_{j_2} \dots k_{j_m} \right| \left| \frac{\partial}{\partial a_{j_1}} \frac{\partial}{\partial b_{j_2}} \cdots \frac{\partial}{\partial k_{j_m}} \right| \right] A a_{i_1} \dots k_{i_m};$$

for all terms of the Σ, except the one first quoted, give zero when operating on the term chosen.

If $m<n$, $H=0$, and $\{\mathrm{ab} \dots \mathrm{k}\}'f = 0$; for every term of f must contain at least two variables with the same indices.

Now consider any function F homogeneous but no longer linear in the variables of each set, having n sets and m variables in each set. Then we form from F a function f, as shown above, such that we may consider, instead of F,

$$P = \frac{1}{\alpha!\, \beta! \dots \kappa!} \{\mathrm{a}^{(1)} \mathrm{a}^{(2)} \dots \mathrm{a}^{(\alpha)}\} \{\mathrm{b}^{(1)} \dots \mathrm{b}^{(\beta)}\} \dots$$

$$\dots \{\mathrm{k}^{(1)} \dots \mathrm{k}^{(\kappa)}\} f(a^{(1)}, a^{(2)}, \dots, a^{(\alpha)}, b^{(1)}, \dots, k^{(\kappa)}).$$

Then, if $H_{a^{(1)} b^{(1)} \dots k^{(1)}}$ be what H becomes when we write in it the sets $a^{(1)}, b^{(1)}, \dots, k^{(1)}$ instead of the sets $a, b, \dots, k$, HF becomes

$$\sum_{\alpha_i=1}^{\alpha_i=\alpha} \sum_{\beta_i=1}^{\beta_i=\beta} \cdots \sum_{\kappa_i=1}^{\kappa_i=\kappa} H_{a^{(\alpha_i)} b^{(\beta_i)} \dots k^{(\kappa_i)}} P;$$

this last expression being $= HF$ when we write

$$a^{(1)} = a^{(2)} = \dots = a^{(\alpha)} = a,$$

$$b^{(1)} = b^{(2)} = \dots = b^{(\beta)} = b,$$

$$\dots \quad \dots \quad \dots \quad \dots$$

$$k^{(1)} = k^{(2)} = \dots = k^{(\kappa)} = k.$$

But $$H_{a^{(\alpha_i)} b^{(\beta_i)} \dots k^{(\kappa_i)}} P = \{\mathrm{a}^{(\alpha_i)} \mathrm{b}^{(\beta_i)} \dots \mathrm{k}^{(\kappa_i)}\} P,$$

as we have already seen; hence in this case

$$\sum_{\alpha_i, \beta_i, \dots, \kappa_i} \{\mathrm{a}^{(\alpha_i)} \mathrm{b}^{(\beta_i)} \dots \mathrm{k}^{(\kappa_i)}\}'$$

is the equivalent of H.

Now, in the substitutional equivalent of H it is assumed that there is a substitutional operator

$$\{a^{(1)}a^{(2)}\dots a^{(\alpha)}\}\{b^{(1)}\dots b^{(\beta)}\}\dots\{k^{(1}\dots k^{(\kappa)}\},$$

of definite form applied to the operand. The same operator may then be attached to this equivalent of H, without affecting the result except as regards a constant. Hence we may write

$$H=\frac{1}{\alpha!\,\beta!\,\dots\,\kappa!}\Sigma\,\{a^{(\alpha_i)}b^{(\beta_i)}\dots k^{(\kappa_i)}\}'\{a^{(1)}\dots a^{(\alpha)}\}\{b^{(1)}\dots b^{(\beta)}\}\dots\{k^{(1)}\dots k^{(\kappa)}\}$$

$$=\frac{1}{\alpha!\,\beta!\dots\kappa!\,(\alpha-1)!\,(\beta-1)!\dots(\kappa-1)!}$$

$$\times\{a^{(1)}\dots a^{(\alpha)}\}\{b^{(1)}\dots b^{(\beta)}\}\dots\{k^{(1)}\dots k^{(\kappa)}\}$$

$$\times\{a^{(1)}b^{(1)}\dots k^{(1)}\}'\{a^{(1)}\dots a^{(\alpha)}\}\{b^{(1)}\dots b^{(\beta)}\}\dots\{k^{(1)}\dots k^{(\kappa)}\}.$$

For $\{a^{(1)}\dots a^{(\alpha)}\}\,\{a^{(1)}b^{(1)}\dots k^{(1)}\}'\,\{a^{(1)}\dots a^{(\alpha)}\}$

$$=\left[1+(a^{(1)}a^{(2)})+(a^{(1)}a^{(3)})+\dots+(a^{(1)}a^{(\alpha)})\right]$$

$$\times\{a^{(2)}\dots a^{(\alpha)}\}\,\{a^{(1)}b^{(1)}\dots k^{(1)}\}'\,\{a^{(1)}\dots a^{(\alpha)}\}$$

$$=(\alpha-1)!\left[1+(a^{(1)}a^{(2)})+\dots+(a^{(1)}a^{(\alpha)})\right]\{a^{(1)}b^{(1)}\dots k^{(1)}\}'\{a^{(1)}\dots a^{(\alpha)}\}$$

$$=(\alpha-1)!\sum_{\alpha_i=1}^{\alpha_i=\alpha}\{a^{(\alpha_i)}b^{(1)}\dots k^{(1)}\}\,\{a^{(1)}\dots a^{(\alpha)}\}.$$

Capelli has shown in the general case how a substitution may be expressed in terms of polar operators; in the case of functions homogeneous and linear in the variables of each set, the effect of a transposition may be obtained thus,

$$D_{ba}D_{ab}f(a,b,c,\dots)=D_{ba}f(b,b,c,\dots)=\{ab\}f(a,b,c,\dots);$$

hence $(ab)\,f(a,b,c,\dots)=(D_{ba}D_{ab}-1)\,f(a,b,c,\dots)$.

Any other substitution operating on f may be expressed as a product of transpositions, and so as a function of polar operators. The converse theorem is also true; for let D_{ab} be a polar operator, operating on a function F of degree α in the variables of the set a, and β in those of the set b; then we consider instead of F the function P

defined as above. The effect of the operator D_{ab} on F is the same as that of

$$\frac{1}{(\beta+1)!}\{\mathrm{b}^{(1)}\mathrm{b}^{(2)}\ldots\mathrm{b}^{(\beta+1)}\}\left[D_{a^{(1)}b^{(\beta+1)}}+D_{a^{(2)}b^{(\beta+1)}}+\ldots+D_{a^{(\alpha)}b^{(\beta+1)}}\right]$$

on P. For each of the sets $a^{(1)}, a^{(2)}, \ldots, a^{(\alpha)}$ in P is in reality equivalent to a, and each of the sets $b^{(1)}, b^{(2)}, \ldots$ equivalent to b. Since P does not contain $b^{(\beta+1)}$,

$$D_{a^{(1)}b^{(\beta+1)}}P=(\mathrm{a}^{(1)}\mathrm{b}^{(\beta+1)})\,P,$$

the right-hand side being no longer a function of $a^{(1)}$.

Now, P is symmetric in the sets $a^{(1)}, \ldots, a^{(\alpha)}$; hence the function $(\mathrm{a}^{(2)}\mathrm{b}^{(\beta+1)})\,P$ is the same as $(\mathrm{a}^{(1)}\mathrm{b}^{(\beta+1)})\,P$, except that $a^{(1)}$ and $a^{(2)}$ are interchanged; hence the function $D_{ab}F$ is equivalent to

$$\frac{\alpha}{(\beta+1)!}\{\mathrm{b}^{(1)}\mathrm{b}^{(2)}\ldots\mathrm{b}^{(\beta+1)}\}\,(\mathrm{a}^{(\alpha)}\mathrm{b}^{(\beta+1)})\,P,$$

which does not contain the set $a^{(\alpha)}$. In this the new set $b^{(\beta+1)}$ may be replaced by the old set $a^{(\alpha)}$ by operating with $(\mathrm{a}^{(\alpha)}\mathrm{b}^{(\beta+1)})$, and the result becomes

$$\frac{\alpha}{(\beta+1)!}\{\mathrm{b}^{(1)}\mathrm{b}^{(2)}\ldots\mathrm{b}^{(\beta)}\mathrm{a}^{(\alpha)}\}\,P,$$

where now $a^{(\alpha)}$ is to be regarded as equivalent to b.

13. If $T_{\alpha,0}\equiv S\{\mathrm{a}_1\mathrm{b}_1\}'\{\mathrm{a}_2\mathrm{b}_2\}'\ldots\{\mathrm{a}_\alpha\mathrm{b}_\alpha\}'\{\mathrm{b}_1\mathrm{b}_2\ldots\mathrm{b}_m\}\,S$

and $\beta>0$, $T_{\alpha,\beta}\equiv S\{\mathrm{a}_1\mathrm{b}_1\}'\{\mathrm{a}_2\mathrm{b}_2\}'\ldots\{\mathrm{a}_\alpha\mathrm{b}_\alpha\}'\{\mathrm{a}_{n-\beta+1}\ldots\mathrm{a}_n\mathrm{b}_1\ldots\mathrm{b}_m\}\,S$,

where $S\equiv\{\mathrm{a}_1\mathrm{a}_2\ldots\mathrm{a}_n\}\{\mathrm{b}_1\mathrm{b}_2\ldots\mathrm{b}_m\}$,

then $T_{0,0}=A_{0,n}\,T_{0,n}+A_{1,n-1}\,T_{1,n-1}+\ldots+A_{n,0}\,T_{n,0}$,

if $m\nless n$; **but, if** $m<n$, the series must stop with $A_{m,n-m}T_{m,n-m}$, and the coefficients A are given by

$$A_{\alpha,\beta}=\binom{\alpha+\beta}{\beta}\frac{m!\,(m+1+\beta-\alpha)}{(m+\beta+1)!}.$$

The theorem to be established is purely formal, an identity between certain substitutional expressions.

When $\alpha<h<n-\beta+1$, the expression

$$S\{\mathrm{a}_1\mathrm{b}_1\}'\{\mathrm{a}_2\mathrm{b}_2\}'\ldots\{\mathrm{a}_\alpha\mathrm{b}_\alpha\}'(a_hb_1)\{\mathrm{a}_{n-\beta+1}\ldots\mathrm{a}_n\mathrm{b}_1\mathrm{b}_2\ldots\mathrm{b}_m\}\,S$$

$$=S\,(\mathrm{a}_h\mathrm{b}_1)\{\mathrm{a}_1\mathrm{a}_h\}'\{\mathrm{a}_2\mathrm{b}_2\}'\ldots\{\mathrm{a}_\alpha\mathrm{b}_\alpha\}'\{\mathrm{a}_{n-\beta+1}\ldots\mathrm{a}_n\mathrm{b}_1\mathrm{b}_2\ldots\mathrm{b}_m\}\,S,$$

for it is well known that, if s be any substitution, $(\mathrm{a}_h\mathrm{b}_1)\,s\,(\mathrm{a}_h\mathrm{b}_1)$ is the same as that substitution obtained from s by the interchange of a_h and b_1; and hence, if U be any substitutional expression,

$$(\mathrm{a}_h \mathrm{b}_1)\, U\, (\mathrm{a}_h \mathrm{b}_1) = U_1,$$

the expression obtained from U by the interchange of a_h and b_1; and hence

$$U\, (\mathrm{a}_h \mathrm{b}_1) = (\mathrm{a}_h \mathrm{b}_1)\, U_1.$$

Now, no one of the factors $\{\mathrm{a}_2 \mathrm{b}_2\}' \ldots \{\mathrm{a}_\alpha \mathrm{b}_\alpha\}' \{\mathrm{a}_{n-\beta+1} \ldots \mathrm{a}_n \mathrm{b}_1 \mathrm{b}_2 \ldots \mathrm{b}_m\}$ contains either of the letters a_1 or a_h; hence

$$\begin{aligned} S\, (\mathrm{a}_h \mathrm{b}_1) \{\mathrm{a}_1 \mathrm{a}_h\}' \{\mathrm{a}_2 \mathrm{b}_2\}' \ldots \{\mathrm{a}_\alpha \mathrm{b}_\alpha\}' \{\mathrm{a}_{n-\beta+1} \ldots \mathrm{a}_n \mathrm{b}_1 \mathrm{b}_2 \ldots \mathrm{b}_m\}\, S & \\ = S\, (\mathrm{a}_h \mathrm{b}_1) \{\mathrm{a}_2 \mathrm{b}_2\}' \ldots \{\mathrm{a}_\alpha \mathrm{b}_\alpha\}' \{\mathrm{a}_{n-\beta+1} \ldots \mathrm{a}_n \mathrm{b}_1 \mathrm{b}_2 \ldots \mathrm{b}_m\} \{\mathrm{a}_1 \mathrm{a}_h\}'\, S & \\ = 0; & \end{aligned}$$

for

$$\{\mathrm{a}_1 \mathrm{a}_h\}' \{\mathrm{a}_1 \mathrm{a}_2 \ldots \mathrm{a}_n\} = 0;$$

and therefore

$$S \{\mathrm{a}_1 \mathrm{b}_1\}' \{\mathrm{a}_2 \mathrm{b}_2\}' \ldots \{\mathrm{a}_\alpha \mathrm{b}_\alpha\}' (\mathrm{a}_h \mathrm{b}_1) \{\mathrm{a}_{n-\beta+1} \ldots \mathrm{a}_n \mathrm{b}_1 \mathrm{b}_2 \ldots \mathrm{b}_m\}\, S = 0.$$

Hence

$$\begin{aligned} T_{\alpha,\beta} &= S \{\mathrm{a}_1 \mathrm{b}_1\}' \{\mathrm{a}_2 \mathrm{b}_2\}' \ldots \{\mathrm{a}_\alpha \mathrm{b}_\alpha\}' \{\mathrm{a}_{n-\beta+1} \ldots \mathrm{a}_n \mathrm{b}_1 \mathrm{b}_2 \ldots \mathrm{b}_m\}\, S \\ &= S \{\mathrm{a}_1 \mathrm{b}_1\}' \ldots \{\mathrm{a}_\alpha \mathrm{b}_\alpha\}' \big[1 + (\mathrm{a}_{n-\beta+1} \mathrm{a}_{n-\beta+2}) + (\mathrm{a}_{n-\beta+1} \mathrm{a}_{n-\beta+3}) + \ldots \\ &\qquad + (\mathrm{a}_{n-\beta+1} \mathrm{a}_n) + (\mathrm{a}_{n-\beta+1} \mathrm{b}_1) + \ldots + (\mathrm{a}_{n-\beta+1} \mathrm{b}_m)\big] \\ &\qquad \times \{\mathrm{a}_{n-\beta+2} \ldots \mathrm{a}_n \mathrm{b}_1 \mathrm{b}_2 \ldots b_m\}\, S \\ &= S \{\mathrm{a}_1 \mathrm{b}_1\}' \ldots \{\mathrm{a}_\alpha \mathrm{b}_\alpha\}' \big[\beta + (\mathrm{a}_{n-\beta+1} \mathrm{b}_{\alpha+1}) + \ldots + (\mathrm{a}_{n-\beta+1} \mathrm{b}_m)\big] \\ &\qquad \times \{\mathrm{a}_{n-\beta+2} \ldots \mathrm{a}_n \mathrm{b}_1 \mathrm{b}_2 \ldots \mathrm{b}_m\}\, S \\ &= S \{\mathrm{a}_1 \mathrm{b}_1\}' \ldots \{\mathrm{a}_\alpha \mathrm{b}_\alpha\}' \big[-(m-\alpha) \{\mathrm{a}_{n-\beta+1} \mathrm{b}_{\alpha+1}\}' + (m+\beta-\alpha)\big] \\ &\qquad \times \{\mathrm{a}_{n-\beta+2} \ldots \mathrm{a}_n \mathrm{b}_1 \mathrm{b}_2 \ldots \mathrm{b}_m\}\, S \\ &= -(m-\alpha)\, T_{\alpha+1,\beta-1} + (m+\beta-\alpha)\, T_{\alpha,\beta-1}; \end{aligned}$$

therefore $$T_{\alpha,\beta} = \frac{1}{m+\beta-\alpha+1} T_{\alpha,\beta+1} + \frac{m-\alpha}{m+\beta-\alpha+1} T_{\alpha+1,\beta}.$$

By repeated application of this formula, we obtain

$$\begin{aligned} T_{00} &= \frac{1}{m+1} T_{0,1} + \frac{m}{m+1} T_{1,0} \\ &= \ldots \\ &\ldots \quad \ldots \quad \ldots \quad \ldots \\ &= A_{0,i}\, T_{0,i} + A_{1,i-1}\, T_{1,i-1} + \ldots + A_{i,0}\, T_{i,0}, \end{aligned}$$

except when $i > m$, in which case the series ends with $A_{m,i-m} T_{m,i-m}$; i being supposed to be not greater than n, and the A's being numerical coefficients.

To find these coefficients a recurrence formula is obtained by proceeding from the last line written down a step further. The coefficient of $T_{j,i-j+1}$ in this will be

$$A_{j,i-j+1} = \frac{m-j+1}{m+i-2j+3} A_{j-1,i-j+1} + \frac{1}{m+i-2j+1} A_{j,i-j}.$$

Hence $$A_{\alpha,\beta} = \frac{m-\alpha+1}{m+\beta-\alpha+2} A_{\alpha-1,\beta} + \frac{1}{m+\beta-\alpha} A_{\alpha,\beta-1}.$$

It follows from this that, if

$$A_{\alpha,\beta} = \binom{\alpha+\beta}{\beta} \frac{m!\,(m+1+\beta-\alpha)}{(m+\beta+1)!},$$

when $\alpha < \alpha_1$, and also when $\alpha = \alpha_1$ so long as $\beta < \beta_1$, it is true when $\alpha = \alpha_1$ and $\beta = \beta_1$. Hence, on this hypothesis it is true whenever $\alpha < \alpha_1 + 1$. But this form of $A_{\alpha,\beta}$ is correct, as it is easy to verify, when $\alpha = 0$, and also when $\beta = 0$ and $\alpha < n+1$. Hence it is true always when $\alpha < n+1$. And the theorem is proved.

14. As has been pointed out, the theorem just proved is merely a substitutional identity. If the two sides of the identity be made to operate on the same function, the results must be equal. This operand may be taken to be any function of $m+n$ variables

$$a_1,\ a_2,\ \dots,\ a_n,\quad b_1,\ b_2,\ \dots,\ b_m;$$

or again any function of $m+n$ sets of variables

$$\begin{array}{llll} a_{1,1}, & a_{1,2}, & a_{1,3}, \ \dots, & a_{1,p}, \\ a_{2,1}, & a_{2,2}, & \dots\dots\dots, & a_{2,p}, \\ \dots & \dots & \dots & \dots \\ a_{n,1}, & a_{n,2}, & \dots\dots\dots, & a_{n,p}, \\ b_{1,1}, & b_{1,2}, & \dots\dots\dots, & b_{1,p}, \\ \dots & \dots & \dots & \dots \\ b_{m,1}, & b_{m,2}, & \dots\dots\dots, & b_{m,p}, \end{array}$$

[illegible] interchanging two sets, just as in §§ 10 and 11 [illegible] functions there discussed interchanged two fu[illegible] has been seen in § 11, when the operand F is linear and homogeneous in the variables of each set, the expression $\{\mathrm{a}_1\,\mathrm{b}_1\}'$ is equivalent to H_{a_1, b_1}, where

$$H_{a_1, b_1} = \Sigma \mid a_{1, i_1} \; b_{1, i_2} \mid \; \left| \frac{\partial}{\partial a_{1, i_1}} \; \frac{\partial}{\partial b_{1, i_2}} \right| .$$

(1) Let us take for operand

$$F = a_{1_x} a_{2_x} \ldots a_{n_x} b_{1_y} b_{2_y} \ldots b_{m_y} ,$$

where the factors of F are binary symbolical factors, thus

$$a_{1_x} = a_{1,1} x_1 + a_{1,2} x_2,$$

$$b_{1_y} = b_{1,1} y_1 + b_{1,2} y_2.$$

Then $T_{0,0} F = \{\mathrm{a}_1 \mathrm{a}_2 \ldots \mathrm{a}_n\} \{\mathrm{b}_1 \mathrm{b}_2 \ldots \mathrm{b}_m\} \{\mathrm{b}_1 \ldots \mathrm{b}_m\} \{\mathrm{a}_1 \ldots \mathrm{a}_n\} \{\mathrm{b}_1 \ldots \mathrm{b}_m\} F$

$$= (n!)^2 (m!)^3 F.$$

Denote by D and Δ polar operators, such that, ϕ being homogeneous and of order n in x_1, x_2, and homogeneous and of order m in y_1, y_2, then

$$D\phi = \frac{1}{m} \left(x_1 \frac{\partial \phi}{\partial y_1} + x_2 \frac{\partial \phi}{\partial y_2} \right),$$

$$\Delta\phi = \frac{1}{n} \left(y_1 \frac{\partial \phi}{\partial x_1} + y_2 \frac{\partial \phi}{\partial x_2} \right),$$

also let

$$\Omega\phi = \frac{1}{mn} \left(\frac{\partial^2 \phi}{\partial x_1 \partial y_2} - \frac{\partial^2 \phi}{\partial x_2 \partial y_1} \right);$$

these being the operators used by Clebsch (*Binaren Formen*, pp. 13, 14, *et seq.*).

Then $$D^m F = a_{1_x} a_{2_x} \ldots a_{n_x} b_{1_x} b_{2_x} \ldots b_{m_x},$$

and the effect of operating with Δ^m on this function is to change it to the sum of all possible terms obtained from $D^m F$ by writing y for x in m of its factors, divided by their number. But this is the same as

$$\frac{1}{(m+n)!} \{\mathrm{a}_1 \mathrm{a}_2 \ldots \mathrm{a}_n \mathrm{b}_1 \mathrm{b}_2 \ldots \mathrm{b}_m\} \, a_{1_x} a_{2_x} \ldots a_{n_x} b_{1_y} b_{2_y} \ldots b_{m_y}.$$

Hence

$$T_{0,n} F = \{\mathrm{a}_1 \ldots \mathrm{a}_n\} \{\mathrm{b}_1 \ldots \mathrm{b}_m\} \{\mathrm{a}_1 \ldots \mathrm{a}_n \mathrm{b}_1 \ldots \mathrm{b}_m\} \{\mathrm{a}_1 \ldots \mathrm{a}_n\} \{\mathrm{b}_1 \ldots \mathrm{b}_m\} F$$

$$= (n!)^2 (m!)^2 \{\mathrm{a}_1 \ldots \mathrm{a}_n \mathrm{b}_1 \ldots \mathrm{b}_m\} F$$

$$= (n!)^2 (m!)^2 (m+n)! \, \Delta^m D^m F.$$

Again,

$$\Omega F = \frac{1}{mn} \sum_{i=1}^{i=n} \sum_{j=1}^{j=m} (a_i b_j)\, a_{1_r} \dots a_{i-1_x}\, a_{i+1_x} \dots a_{n_x}\, b_{1_y} \dots b_{j-1_y} b_{j+1_y} \dots b_{m_y};$$

and $$D^{m-1}\Omega F = \frac{1}{mn} \sum_i \sum_j (a_i b_j)\, a_{1_x} \dots a_{i-1_x}\, a_{i+1x}\, a_{n_x} b_{1_x} \dots b_{j-1_x} b_{j+1_x} \dots b_{m_x}.$$

And $\Delta^{m-1}D^{m-1}\Omega F$ is equal to the sum of all possible terms obtained by substituting y for x in $m-1$ of the factors of each term of $D^{m-1}\Omega F$ divided by their number

$$= \frac{1}{(m+n-2)!}\, \frac{1}{mn} \sum_{i,j} (a_i b)\, \{\mathbf{a}_1 \dots \mathbf{a}_{i-1}\, \mathbf{a}_{i+1} \dots \mathbf{a}_n \mathbf{b}_1 \dots \mathbf{b}_{j-1}\, \mathbf{b}_{j+1} \dots \mathbf{b}_m\}$$
$$\times\, a_{1_x} \dots a_{i-1_x} a_{i+1_x} \dots a_{n_x}\, b_{1_y} \dots b_{j-1_y} b_{j+1_y} \dots b_{m_y}$$

$$= \frac{1}{(m+n-2)!}\, \frac{1}{m!\, n!} \{\mathbf{a}_1 \mathbf{a}_2 \dots \mathbf{a}_n\}\, \{\mathbf{b}_1 \mathbf{b}_2 \dots \mathbf{b}_m\}\, (a_1 b_1)\, \{\mathbf{a}_2 \dots \mathbf{a}_n\, \mathbf{b}_2 \dots \mathbf{b}_m\}$$
$$\times\, a_2\, \dots a_{n_x}\, b_{2_y} \dots b_{m_y}.$$

Hence

$$\begin{aligned}
T_{1,\,n-1} F &= S\,\{\mathbf{a}_1 \mathbf{b}_1\}'\, \{\mathbf{a}_2 \dots \mathbf{a}_n\, \mathbf{b}_1 \dots b_m\}\, SF \\
&= n!\; m!\, S\,\{\mathbf{a}_1 \mathbf{b}_1\}'\, \{\mathbf{a}_2 \dots \mathbf{a}_n\, \mathbf{b}_1 \dots \mathbf{b}_m\}\, a_{1_r} \dots a_{n_x}\, b_{1_y} \dots b_{m_y} \\
&= n!\; m!\, S\{\mathbf{a}_1 \mathbf{b}_1\}' \big[m a_{1_x} b_{1_y} \{\mathbf{a}_2 \dots \mathbf{a}_n\, \mathbf{b}_2 \dots \mathbf{b}_m\}\, a_{2_x} \dots a_{nx}\, b_{2_y} \dots b_{m_y} \\
&\qquad + (n-1)\, a_1\;\, b_{1_x} \{\mathbf{a}_2 \dots \mathbf{a}_n \mathbf{b}_2 \dots \mathbf{b}_m\}\, a_{2_x} \dots a_{(n-1)_x} a_{n_y}\, b_{2_y} \dots b_{m_y} \big] \\
&= n!\; m!\; mS\, (a_1 b_1)\, (xy)\, \{\mathbf{a}_2 \dots \mathbf{a}_n\, \mathbf{b}_2 \dots \mathbf{b}_m\}\, a_{2_x} \dots a_{n_x}\, b_2\; \dots b_{m_y} \\
&= (xy)\, (n!)^2\, (m!)^2\, (m+n-2)!\; m\Delta^{m-1} D^{m-1}\Omega F.
\end{aligned}$$

Proceeding in the same way,

$$\Omega^h F = \frac{(m-h)!\,(n-h)!}{m!\; n!} \sum (a_1 b_1)(a_2 b_2) \dots (a_h b_h)\, a_{h+1_x} \dots a_{n_x}\, b_{h+1_y} \dots b_{m_y},$$

$D^{m-h}\Omega^h F$

$$= \frac{(m-h)!\,(n-h)!}{m!\; n!} \sum (a_1 b_1)(a_2 b_2) \dots (a_h b_h)\, a_{h+1_x} \dots a_{n_x}\, b_{h+1_y} \dots b_{m_x},$$

$\Delta^{m-h} D^{m-h}\Omega^h F$

$$= \frac{1}{(m+n-2h)!}\, \frac{1}{m!\; n!} \{\mathbf{a}_1 \mathbf{a}_2 \dots \mathbf{a}_n\} \{\mathbf{b}_1 \dots \mathbf{b}_m\}\, (a_1 b_1)(a_2 b_2) \dots (a_h b_h)$$
$$\times\, \{\mathbf{a}_{h+1} \dots \mathbf{a}_n\, \mathbf{b}_{h+1} \dots \mathbf{b}_m\}\, a_{h+1_x} \dots a_{n_x}\, b_{h+1_y} \dots b_{m_y}.$$

And hence

$$T_{h,\,n-h}F = S\,\{\mathrm{a}_1\mathrm{b}_1\}'\,\{\mathrm{a}_2\mathrm{b}_2\}'\ldots\{\mathrm{a}_h\mathrm{b}_h\}'\{\mathrm{a}_{h+1}\ldots\mathrm{a}_n\,\mathrm{b}_1\ldots\mathrm{b}_m\}\,SF$$

$$= n!\;m!\;S\{\mathrm{a}_1\mathrm{b}_1\}'\ldots\{\mathrm{a}_h\mathrm{b}_h\}'\Big[\frac{m!}{(m-h)!}\,a_{1_x}\ldots a_{h_x}\,b_{1_y}\ldots b_{h_y}$$

$$\times\{\mathrm{a}_{h+1}\ldots\mathrm{a}_n\,\mathrm{b}_{h+1}\ldots\mathrm{b}_m\}\,a_{h+1_x}\ldots a_{n_x}b_{h+1_y}\ldots b_{m_y}+P\Big],$$

where P contains the product $a_{i_x}b_{i_x}$ for some value of i between 1 and h inclusive, and hence is annihilated by the product $\{\mathrm{a}_1\mathrm{b}_1\}'\ldots\{\mathrm{a}_h\mathrm{b}_h\}'$; therefore

$$T_{h,\,n-h}F = (xy)^h\,n!\,m!\,\frac{m!}{(m-h)!}\,S\,(a_1b_1)\ldots(a_hb_h)\,\{\mathrm{a}_{h+1}\ldots\mathrm{a}_n\,\mathrm{b}_{h+1}\ldots\mathrm{b}_m\}$$

$$\times\,a_{h+1_x}\ldots a_{n_x}\,b_{h+1_y}\ldots b_{m_y}$$

$$= (xy)^h\,(n!)^2\,(m!)^2\,(m+n-2h)!\,\frac{m!}{(m-h)!}\,\Delta^{m-h}D^{m-h}\Omega^hF;$$

and hence $$A_{h,\,n-h}\,T_{h,\,n-h}\,F$$

$$= (xy)^h\binom{n}{h}\frac{m!\,(m+1+n-2h)}{(m+n-h+1)!}\,(n!)^3\,(m!)^2\,(m+n-2h)!\,\frac{m!}{(m-h)!}$$

$$\times\,\Delta^{m-h}D^{m-h}\Omega^h\,F$$

$$= (n!)^2\,(m!)^3\,\frac{\binom{n}{h}\binom{m}{h}}{\binom{m+n-h+1}{h}}\,(xy)^h\,\Delta^{m-h}D^{m-h}\Omega^hF.$$

Hence we obtain Gordan's series

$$F = \sum_{h=0}^{h=m}\frac{\binom{n}{h}\binom{m}{h}}{\binom{m+n-h+1}{h}}\,(xy)^h\,\Delta^{m-h}D^{m-h}\Omega^hF,$$

if $n \geqslant m$; if $n<m$, the summation must be taken from $h=0$ to $h=n$.

(2) Let F as before $= a_{1_x}a_{2_x}\ldots a_{n_x}b_{1_y}b_{2_y}\ldots b_{m_y}$, where the factors of F are now ternary symbolical factors, thus

$$a_{1_x} = a_{1,1}x_1 + a_{1,2}x_2 + a_{1,3}x_3.$$

Then $$T_{0,0}F = (n!)^2\,(m!)^3\,F,$$

and $$T_{0,n}F = (n!)^2(m!)^2(m+n)!\,\Delta^mD^mF,$$

just as when the factors of F were binary; the definition of Δ and D being that, if ϕ is a function homogeneous and of order n in x_1, x_2, x_3, and homogeneous and of order m in y_1, y_2, y_3, then

$$D\phi = \frac{1}{m}\left(x_1\frac{\partial\phi}{\partial y_1}+x_2\frac{\partial\phi}{\partial y_2}+x_3\frac{\partial\phi}{\partial y_3}\right),$$

$$\Delta\phi = \frac{1}{n}\left(y_1\frac{\partial\phi}{\partial x_1}+y_2\frac{\partial\phi}{\partial x_2}+y_3\frac{\partial\phi}{\partial x_3}\right).$$

Let u_1, u_2, u_3 be three quantities defined by

$$u_1 = x_2y_3-x_3y_2,$$

$$u_2 = x_3y_1-x_1y_3,$$

$$u_3 = x_1y_2-x_2y_1;$$

then $$a_xb_y-a_yb_x = (abu);$$

and, just as in the former case,

$$T_{h,\,n-h}F = n!\,m!\,S\{\mathrm{a}_1\mathrm{b}_1\}'\ldots\{\mathrm{a}_h\mathrm{b}_h\}'\frac{m!}{(m-h)!}a_{1_x}\ldots a_{h_x}\,b_{1_y}\ldots b_{h_y}$$
$$\times\{\mathrm{a}_{h+1}\ldots\mathrm{a}_n\,\mathrm{b}_{h+1}\ldots\mathrm{b}_m\}\,a_{h+1_x}\ldots a_{n_x}\,b_{h+1_y}\ldots b_{m_y}$$
$$= n!\,m!\frac{m!}{(m-h)!}S(a_1b_1u)\ldots(a_hb_hu)(m+n-2h)!\,\Delta^{m-h}D^{m-h}$$
$$\times a_{h+1_x}\ldots a_{n_x}\,b_{h+1_y}\ldots b_{m_y}.$$

Let us now suppose that $F = a_x^nb_y^m$, and that we may write

$$a_1 = a_2 = \ldots = a_n = a, \quad b_1 = b_2 = \ldots = b_m = b,$$

after all the substitutional operations have been performed on F; then

$$T_{h,\,n-h}F = (n!)^2(m!)^2\frac{m!}{(m-h)!}(m+n-2h)!\,(abu)^h\Delta^{m-h}D^{m-h}a_x^{n-h}b_y^{m-h},$$

and, as in the case of Gordan's series, we obtain

$$a_x^nb_y^m = \sum_{h=0}^{h=m}\frac{\binom{n}{h}\binom{m}{h}}{\binom{m+n-h+1}{h}}(abu)^h\Delta^{m-h}D^{m-h}a_x^{n-h}b_y^{m-h},$$

[illegible] $n < m$, the summation must be taken from $h=0$ to $h=n$. [illegible] may be established in exactly the same way if a_x, b_y [illegible] factors, provided we write instead of (abu) the [illegible]

(3) The series furnishes information concerning those functions F which satisfy the substitutional equations

$$\begin{aligned} \{a_1 b_1 b_2 \ldots b_m\}\, F &= 0, \\ \{a_2 b_1 b_2 \ldots b_m\}\, F &= 0, \\ \ldots \quad \ldots \quad &\ldots \quad \ldots \\ \{a_n b_1 b_2 \ldots b_m\}\, F &= 0. \end{aligned}$$

For in this case $T_{\alpha,\beta} F = 0$, provided $\beta > 0$.

Hence

$$n!\,(m!)^2\,\{a_1 a_2 \ldots a_n\}\,\{b_1 b_2 \ldots b_m\}\, F = T_{0,0}\, F = \frac{m+1-n}{m+1}\, T_{n,0} F \quad \text{or} = 0$$

according as $m+1$ is or is not greater than n. When n is greater than m,

$$\{a_1 a_2 \ldots a_{m+1}\}\,\{b_1 b_2 \ldots b_m\}\, F = 0.$$

15. Let the letters $a_1, a_2, \ldots, a_n$ be arranged in any manner in horizontal rows, so that each row has its first letter in the same vertical column, its second letter in a second vertical column, and so on, and so that no row contains more letters than any row above it; then form the substitutional expression

$$S = \Gamma'_1 \Gamma'_2 \ldots \Gamma'_h\, G_1 G_2 \ldots G_k,$$

such that Γ'_1 is the negative symmetric group of the letters of the first row, Γ'_2 that of the letters of the second row, and so on, Γ'_h being that of the letters of the last row; and that G_1 is the positive symmetric group of the letters of the first column, G_2 that of the letters of the second column, and so on, G_k being that of the letters of the last column (it being understood, in case a row or column contains only one letter, that the positive or negative symmetric group of a single letter is unity). Then, if $T_{\alpha_1, \alpha_2, \ldots, \alpha_h}$ be the sum of all expressions S formed as above from all possible tabular arrangements of the letters, so that there are α_1 letters in the first row, α_2 in the second, and so on, the α's satisfying

$$\alpha_1 + \alpha_2 + \ldots + \alpha_h = n,$$

and

$$\alpha_1 \nless \alpha_2 \nless \alpha_3 \ldots \nless \alpha_h,$$

it is possible to uniquely determine numerical coefficients $A_{\alpha_1, \alpha_2, \ldots, \alpha_h}$ so that

$$1 = \Sigma A_{\alpha_1, \alpha_2, \ldots, \alpha_h}\, T_{\alpha_1, \alpha_2, \ldots, \alpha_h},$$

where the Σ extends to all possible positive integral values of $\alpha_1, \alpha_2, \ldots, \alpha_h$ which satisfy the two conditions just laid down, the number h of α's not being fixed.

Let us suppose the terms T to be arranged in order, so that $T_{\alpha_1, \alpha_2, \ldots, \alpha_h}$ will come before $T_{\beta_1, \beta_2, \ldots, \beta_{h'}}$, if $\alpha_1 < \beta_1$, or if $\alpha_1 = \beta_1$, but $\alpha_2 < \beta_2$, or if $\alpha_1 = \beta_1$, $\alpha_2 = \beta_2$, ..., $\alpha_{i-1} = \beta_{i-1}$, but $\alpha_i < \beta_i$.

Consider one of the expressions S of which $T_{\alpha_1, \alpha_2, \ldots, \alpha_h}$ is the sum, and the table of letters from which S is formed. Let N be the product of the negative symmetric groups of S, and P the product of its positive symmetric groups, so that

$$S = NP.$$

The degrees of the groups in N are $\alpha_1, \alpha_2, \ldots, \alpha_h$; the degrees of the groups in P depend solely on these numbers, as may be seen from the table, for these groups are formed by the vertical columns in the table. Thus there are only h rows, so that there cannot be more than h elements in any column; in the first α_h columns there are exactly h elements, since the number of letters α_h in the last row is not greater than that in any row above. Next, there are $\alpha_{h-1} - \alpha_h$ columns containing exactly $h-1$ elements, and so on. Hence in P there are first α_h groups of degree h, then $\alpha_{h-1} - \alpha_h$ groups of degree $h-1$, and so on, there being α_1 groups altogether.

Let Γ' be any negative symmetric group which contains a pair of letters out of some one column in the table for S; then $P\Gamma' = 0$, for P contains this pair of letters in a positive symmetric group; and always, as has been seen in § 10,

$$\{\mathrm{abcd} \ldots\}\{\mathrm{abc'd'} \ldots\} = 0.$$

Again, if Γ' be of degree greater than α_1, then it must contain a pair of letters out of some one column in the table for S, for there are only α_1 different columns. Hence, if the degree of Γ' is greater than α_1, $P\Gamma' = 0$.

Now, let S_1 be one of the expressions of which $T_{\beta_1, \beta_2, \ldots, \beta_{h'}}$ is the sum, where $T_{\beta_1, \beta_2, \ldots, \beta_{h'}}$ is a term which comes after the term $T_{\alpha_1, \alpha_2, \ldots, \alpha_h}$ when these terms are arranged in order; and let

$$S_1 = N_1 P_1,$$

where N_1 is the product of the negative symmetric groups of S_1, and P_1 that of the positive symmetric groups. Then

$$PN_1 = 0.$$

For, if $\beta_1 > \alpha_1$, N_1 contains a negative symmetric group Γ' of degree greater than α_1; and hence, as we have seen,

$$P\Gamma' = 0,$$

and therefore $$PN_1 = 0.$$

Now, since $T_{\beta_1, \beta_2, \dots, \beta_{h'}}$ comes after $T_{\alpha_1, \alpha_2, \dots, \alpha_h}$, then $\beta_1 > \alpha_1$; or $\beta_1 = \alpha_1$ and $\beta_2 > \alpha_2$; or $\beta_1 = \alpha_1$, $\beta_2 = \alpha_2$, ..., $\beta_{i-1} = \alpha_{i-1}$, but $\beta_i > \alpha_i$.

Let $$N_1 = \Gamma'_{\beta_1}\Gamma'_{\beta_2}\dots\Gamma'_{\beta_{h'}},$$

the degrees of the different groups being equal to their suffixes. Suppose that $\beta_1 = \alpha_1$, and that Γ'_{β_1} contains no pair of letters which occur in any one column of the table for S (otherwise $PN_1 = 0$), and that $\beta_2 > \alpha_2$. Then Γ'_{β_1} contains one letter belonging to each of the columns, that is, one letter belonging to each of the $\beta_1 = \alpha_1$ groups of P. We will for the moment suppress all these letters belonging to Γ'_{β_1}. When this is done, let P become P', N_1 become N_1'; then P' and N_1' are related in exactly the same way as P and N_1 are. Thus there are only α_2 groups in P', and α_2 columns in the table which gives P', for one letter from each group or column has been suppressed, and thus $\alpha_1 - \alpha_2$ groups have gone altogether. But all the β_2 letters of Γ'_{β_2} occur in the table for P'; and, since $\beta_2 > \alpha_2$, some one of the α_2 columns of P' must contain more than one of the letters of Γ'_{β_2}; hence

$$P'\Gamma'_{\beta_2} = 0.$$

But P is obtained from P' by adding α_1 new letters to its groups; and hence, if one of the groups of P' has a pair of letters in common with Γ'_{β_2}, the same is true for P; and therefore

$$P\Gamma'_{\beta_2} = 0,$$

and $$PN_1 = 0.$$

The argument is exactly the same in the general case

$$\beta_1 = \alpha_1,\ \beta_2 = \alpha_2,\ \dots,\ \beta_{i-1} = \alpha_{i-1},\ \beta_i > \alpha_i.$$

The letters of each of the groups $\Gamma'_{\beta_1}, \Gamma'_{\beta_2}, \dots, \Gamma'_{\beta_{i-1}}$ are suppressed, it being supposed that

$$P\Gamma_{\beta_1}\Gamma'_{\beta_2}\dots\Gamma'_{\beta_{i-1}}$$

does not vanish. Then, if P and N_1 become P' and N_1', these products are related to each other in the same way as P and N_1, and the necessary consequence of $\beta_i > \alpha_i$ becomes

$$P'N_1' = 0,$$

for there is a group in N_1' which contains more letters than there are different columns in the table for P', and hence it must contain a pair of letters from the same column. Then P and N are obtained from P' and N_1' by adding new letters and new groups; but the letters in P' and N_1' are left undisturbed. Hence, if

$$P'N_1' = 0,$$

then
$$PN_1 = 0.$$

Hence, provided $T_{\beta_1, \beta_2, \ldots, \beta_{h'}}$ comes after $T_{\alpha_1, \alpha_2, \ldots, \alpha_h}$, when the terms are arranged in order,

$$PN_1 = 0;$$

and hence
$$PS_1 = PN_1P_1 = 0,$$

and
$$PT_{\beta_1, \beta_2, \ldots, \beta_{h'}} = P.\Sigma S_1 = 0;$$

therefore
$$NP.T_{\beta_1, \beta_2, \ldots, \beta_{h'}} = 0,$$

and
$$T_{\alpha_1, \alpha_2, \ldots, \alpha_h} T_{\beta_1, \beta_2, \ldots, \beta_{h'}} = (\Sigma NP)\, T_{\beta_1, \beta_2, \ldots, \beta_{h'}} = 0.$$

Let $t_{\alpha_1, \alpha_2, \ldots, \alpha_h}$ represent the sum of all those substitutions of the group $\{a_1 a_2 \ldots a_n\}$ which are formed of h cycles of orders $\alpha_1, \alpha_2, \ldots, \alpha_h$ respectively. Then, from the way in which $T_{\alpha_1, \alpha_2, \ldots, \alpha_h}$ is formed, viz., as the sum of the expressions obtained when the letters in the table are permuted in any way, but so that the number of letters in any row or column is unchanged, it follows that $T_{\alpha_1, \alpha_2, \ldots, \alpha_h}$ is a function of the expressions $t_{\beta_1, \beta_2, \ldots, \beta_{h'}}$ only. That is, if it contains any one substitution s multiplied by some constant, it contains every substitution similar to s multiplied by the same constant. Hence

$$T_{\alpha_1, \alpha_2, \ldots, \alpha_h} = \Sigma \lambda_{\beta_1, \beta_2, \ldots, \beta_{h'}} t_{\beta_1, \beta_2, \ldots, \beta_{h'}},$$

where the λ's are constants.

Consider the coefficient of the identical substitution in the product

$$T_{\alpha_1, \alpha_2, \ldots, \alpha_h} . T_{\alpha_1, \alpha_2, \ldots, \alpha_h} \equiv T^2_{\alpha_1, \alpha_2, \ldots, \alpha_h}.$$

To obtain it we have to multiply each term λs of the first T by the term $\lambda' s^{-1}$, involving the inverse substitution, in the second factor. But every substitution is similar to its own inverse, and therefore, if s is a term of $t_{\beta_1, \beta_2, \ldots, \beta_{h'}}$, s^{-1} is also a term of this expression. It follows from the form just found for $T_{\alpha_1, \alpha_2, \ldots, \alpha_h}$ that the coefficients of s and s^{-1} are the same. Consequently the coefficient of the identical substitution in $T^2_{a_1, a_2, \ldots, a_h}$ is

$$\Sigma \mu \lambda^2_{\beta_1, \beta_2, \ldots, \beta_{h'}},$$

where μ is the number of different substitutions in the sum

$$t_{\beta_1, \beta_2, \ldots, \beta_{h'}}.$$

Now, every term of $\Sigma \mu \lambda^2_{\beta_1, \beta_2, \ldots, \beta_{h'}}$ is essentially positive, for no unreal quantities can occur in the formation of T; this coefficient cannot then be zero. Consequently $T^2_{a_1, a_2, \ldots, a_h}$ does not vanish identically.

We can now prove that no relation exists between the T's; for, suppose that one such exists, of which the first term when the T's are arranged according to their proper order is $\lambda T_{a_1, a_2, \ldots, a_h}$. Multiply this equation by $T_{a_1, a_2, \ldots, a_h}$; then every term but the first vanishes: for $TT' = 0$ if T' comes after T. Hence

$$\lambda T^2_{a_1, a_2, \ldots, a_h} = 0;$$

and therefore, by what we have just proved, $\lambda = 0$. Hence $T_{a_1, a_2, \ldots, a_h}$ cannot be the first term, and the relation is impossible.

The expression $t_{a_1, a_2, \ldots, a_h}$ has been defined as the sum of all the substitutions of the group $\{\mathrm{a}_1 \mathrm{a}_2 \ldots \mathrm{a}_n\}$ which are formed of cycles whose orders are $a_1, a_2, \ldots, a_h$ respectively; if cycles order 1 are taken into consideration, the condition

$$a_1 + a_2 + \ldots + a_h$$

may be introduced. Further, the order of the a's in the suffixes of $t_{a_1, a_2, \ldots, a_h}$ is immaterial, so that they may be supposed to be in descending order of magnitude. Then $t_{a_1, a_2, \ldots, a_h}$ thus defined depends on exactly the same numbers as $T_{a_1, a_2, \ldots, a_h}$; hence there are the same number of expressions t as expressions T. Moreover, every T can be expressed in terms of the t's, and no relation can exist between the T's alone; so that we have the same number of independent linear equations as unknown quantities $t_{a_1, a_2, \ldots, a_h}$. It is then possible to solve; hence in general

$$t_{a_1, a_2, \ldots, a_h} = \Sigma \mu_{\beta_1, \beta_2, \ldots, \beta_{h'}} \,.\, T_{\beta_1, \beta_2, \ldots, \beta_{h'}},$$

where μ is numerical; and therefore in particular

$$1 = t_{1, 1, 1, \ldots, 1} = \Sigma A_{a_1, a_2, \ldots, a_h} \,.\, T_{a_1, a_2, \ldots, a_h}.$$

16. For $n = 2, 3, 4$, the work of finding the coefficients of the series by direct calculation is not too laborious: the results are

$$n = 2, \quad 1 = \tfrac{1}{2}\{a_1a_2\} + \tfrac{1}{2}\{a_1a_2\}';$$

$$n = 3, \quad 1 = \frac{1}{3!}\{a_1a_2a_3\} + \frac{1}{9}\Sigma\{a_1a_2\}'\{a_1a_3\} + \frac{1}{3!}\{a_1a_2a_3\}';$$

$$\begin{aligned} n = 4, \quad 1 = \frac{1}{4!}\{a_1a_2a_3a_4\} &+ \frac{1}{32}\Sigma\{a_1a_2\}'\{a_2a_3a_4\} \\ &+ \frac{1}{36}\Sigma\{a_1a_2\}'\{a_3a_4\}'\{a_2a_3\}\{a_1a_4\} \\ &+ \frac{1}{32}\Sigma\{a_1a_2a_3\}'\{a_3a_4\} + \frac{1}{4!}\{a_1a_2a_3a_4\}'. \end{aligned}$$

It is worthy of remark too that, if N be the product of the negative and P that of the positive symmetric groups of one of the expressions of which T is the sum, then

$$T = \Sigma NP = \Sigma PN.$$

For
$$T = \Sigma NP = \lambda\Sigma PNP = \Sigma PN,$$

since PNP is equal to a numerical multiple of

$$(\Sigma N)\,P,$$

where ΣN is the sum of the different expressions obtained from N by operating on N with all the substitutions of P; for it was shown in § 10 that, if $S\,[a_1b_1b_2 \ldots b_m]$ is any substitutional expression affecting the letters $a_1, b_1, b_2, \ldots, b_m$,

$$\{a_1a_2 \ldots a_n\}\,S\,[a_1b_1 \ldots b_m]\,\{a_1 \ldots a_n\}$$
$$= (n-1)!\,\big[\Sigma S\,[a_1, b_1, \ldots b_m]\big]\,\{a_1 \ldots a_n\},$$

the result stated here being an extension of this. In the same way, PNP is the same multiple of

$$P\,(\Sigma N).$$

It is easy now to show that, if T and T' be any two different terms of the sum of § 15, then

$$T\,.\,T' = 0.$$

For, let
$$T = \Sigma NP, \quad T' = \Sigma N'P';$$

then, if T comes before T' in the series, it has been shown already that

$$T.T' = 0.$$

Suppose, then, that T comes after T'; then

$$T.T' = [\Sigma NP][\Sigma N'P']$$

$$= [\Sigma PN][\Sigma P'N'];$$

but in this case

$$NP' = 0;$$

hence $$TT' = 0,$$

whenever T and T' are different.

Multiply now the series of § 15 by

$$T_{\alpha_1, \alpha_2, \ldots, \alpha_h};$$

we then obtain $T_{\alpha_1, \alpha_2, \ldots, \alpha_h} = A_{\alpha_1, \alpha_2, \ldots, \alpha_h} . T^2_{\alpha_1, \alpha_2, \ldots \alpha_h}$.

17. The theorem of § 15, like that of § 13, is purely a substitutional identity; algebraic theorems may be deduced from it by suitably choosing the operand.

(1) *Capelli's Theorem.* — Let the operand be the function $f(a_1, a_2, \ldots, a_n)$ of the n sets of variables

$$\begin{array}{cccc} a_{1,1}, & a_{1,2}, & \ldots, & a_{1,m}, \\ a_{2,1}, & a_{2,2}, & \ldots, & a_{2,m}, \\ \ldots & \ldots & & \ldots \\ a_{n,1}, & a_{n,2}, & \ldots, & a_{n,m}, \end{array}$$

homogeneous and linear in the m variables of each set, such as was under discussion in § 12.

Let $\{\mathfrak{a}_1 \mathfrak{a}_2 \ldots \mathfrak{a}_a\}$ be the positive symmetric group of a of the sets; then

$$\{\mathfrak{a}_1 \mathfrak{a}_2 \ldots \mathfrak{a}_a\} f(a_1, a_2, \ldots, a_n)$$

may be obtained by means of polar operations only from the function

$$f(a_1, a_1, \ldots, a_1, a_{a+1}, a_{a+2}, \ldots, a_n).$$

For, if $\lambda a_{1,r_1} a_{2,r_2} \ldots a_{a,r_a} a_{a+1,r_a+1} \ldots a_{n,r_n}$ be any term of f, then

$$\{\mathfrak{a}_1 \mathfrak{a}_2 \ldots \mathfrak{a}_a\} \lambda a_{1,r_1} a_{2,r_2} \ldots a_{a,r_a} \ldots a_{n,r_n}$$

$$= D_{a_1 a_2} D_{a_1 a_3} \ldots D_{a_1 a_a} \lambda a_{1,r_1} a_{1,r_2} \ldots a_{1,r_a} a_{a+1,r_{a+1}} \ldots a_{n,rn},$$

where D_{xy} is Capelli's operator

$$y_1 \frac{\partial}{\partial x_1} + y_2 \frac{\partial}{\partial x_2} + \ldots + y_m \frac{\partial}{\partial x_m}.$$

Hence $\{a_1 a_2 \ldots a_a\} f = D_{a_1 a_2} D_{a_1 a_3} \ldots D_{a_1 a_a} D_{a_2 a_1} D_{a_3 a_1} \ldots D_{a_a a_1} f.$

And in the same way, if P be the product of β positive symmetric groups no two of which contain the same letter, and which between them contain all the letters $a_1, a_2, \ldots, a_n$, groups of degree unity being taken into account, then Pf is a function which may be obtained by means of polar operations only from a function f_1 which contains only β variables, and f_1 is obtainable by means of polar operations only from f.

Again, it was shown in § 12 that

$$\{a_1 a_2 \ldots a_a\}' f = H_{a_1 a_2 \ldots a_a} f.$$

Hence
$$T_{a_1, a_2, \ldots, a_h} f = \Sigma H_{a_1} H_{a_2} \ldots H_{a_h} \Delta f$$
$$= \Sigma \Delta H_{a_1} H_{a_2} \ldots H_{a_h} f,$$

where, if
$$T = \Sigma NP,$$

H_{a_1} is that H which affects the letters contained in the negative symmetric group degree a_1 of N, H_{a_2} that which affects the letters of the group degree a_2, and so on, and where Δ is the polar operation corresponding to P the form of which we have shown how to find.

If it is required to expand a function $F(x, y, \ldots, u)$ of m sets of variables, there being m variables in each set, which is homogeneous but not linear in the variables of the different sets, we may obtain from this a function

$$f(a_1, a_2, \ldots, a_n)$$

homogeneous and linear in the variables of each of n sets, there being m variables in each set, such that, when we put

$$a_1 = a_2 = \ldots = a_{\rho_1} = x, \quad a_{\rho_1+1} = \ldots = a_{\rho_2} = y, \quad \ldots\ldots, \quad a_n = u,$$

f becomes F; this was shown in § 12. Now, f may be expanded as we have just seen; in the result, the variables of F may be substituted for those of f, and the expansion becomes that for F. This expansion is the same as that obtained by Capelli, and quoted in § 10.

For, if $a_1 < m$, the function $T_{a_1, a_2, \ldots, a_h} f$ may be obtained from f_1 by means of polar operators only, where f_1 is a function of a_1 sets of variables, obtained from f by means of polar operators only. If $a_1 > m$, then

$$T_{a_1, a_2, \ldots, a_h} f = 0.$$

And, if $a_1 = a_2 = \ldots = a_i = m$, $a_{i+1} < m$, then $T_{a_1, a_2, \ldots, a_h} f$ gives rise to a term $| xy \ldots u |^i \phi$, where ϕ is a function obtained from a function of not more than $m-1$ variables by means of polar operations only, which is itself to be obtained by means of polar and Ω operations only from either f or F. For, in the expression P, where

$$\begin{aligned} T_{a_1, a_2, \ldots, a_h} f &= \Sigma P N f \\ &= \Sigma P \,.\, H_{a_1} H_{a_2} \ldots H_{a_h} f, \end{aligned}$$

there are only a_{i+1} groups which affect the letters of

$$\Omega_{a_1} \Omega_{a_2} \ldots \Omega_{a_i} f,$$

where by Ω_a is understood the Ω operator which affects the letters contained in H_a.

The expansion might otherwise be obtained, viz., by considering the function

$$F = a_{1_x} a_{2_x} \ldots a_{\rho_{1_x}} a_{\rho_1 + 1_y} \ldots a_{nu},$$

where the factors of f are m-ary symbolical factors, and then proceeding in a similar manner to that in which Gordan's series was obtained in § 14.

(2) *Peano's Theorem.*[*]—Starting from Capelli's theorem, Peano has proved the following:—"The complete system of concomitants for any number of binary n-ics may be obtained from that for n n-ics by polarization alone; with the one possible exception of that invariant which is the determinant of $n+1$ rows formed by the coefficients of $n+1$ n-ics." He then deduced that the number of concomitant types of a binary n-ic is finite; and proceeded to find the types for a binary cubic, showing that they all give irreducible forms for two cubics because the invariant determinant type referred to above is reducible for the cubic. I have quoted his results for the cubic in my paper, already referred to, on "The Irreducible Concomitants of any Number of Binary Quartics." Peano's theorem may be deduced

---

[*] *Atti di Torino*, t. XVII., p. 580.

directly from that of § 15:—Let F be a type of a binary m-ic of degree n, linear in the coefficients of each of n m-ics; then

$$F = \Sigma A_{a_1, a_2, \dots, a_h} \cdot T_{a_1, a_2, \dots, a_h} F.$$

If $a_1 > m+1$, $T_{a_1, a_2, \dots, a_h} F = 0$; if $a_1 = m+1$, $T_{a_1, a_2, \dots, a_h} F$ is the sum of terms each one of which has for a factor the determinant of $m+1$ rows formed from the coefficients of $m+1$ of the m-ics, and is in consequence reducible. If $a_1 < m+1$, then

$$T_{a_1, a_2, \dots, a_h} F = [\Sigma PN]\, F,$$

where P is the product of a_1 positive symmetric groups, no two of which contain a common element, and which between them contain all the letters $a_1, a_1, \dots, a_n$; it being possible that one or more of these groups is of degree unity. In this case PNF is a function obtained by polarization from a function F_1 of only a_1 sets of variables, where F_1 is a function obtained by polarization from F, as has been proved already. Hence $T_{a_1, a_2, \dots, a_h} F$ is reducible, unless F gives an irreducible concomitant for a_1 m-ics; for concomitants obtained by polarization from reducible concomitants are themselves reducible. Hence, if F is a type of a binary m-ic, which gives no irreducible concomitant for m m-ics, it is reducible, unless F is the determinant of $m+1$ rows formed by the coefficients of $m+1$ of the m-ics. Now, if $a_1 = m$, then

$$T_{a_1, a_2, \dots, a_h} F = [\Sigma \Gamma'_{a_1} S_1]\, F,$$

where Γ'_{a_1} is the negative symmetric group degree a_1 in each of the expressions $\Gamma'_{a_1} S_1$ of which T is the sum. But it has been shown, § 8, that, if Φ be a concomitant type of a binary m-ic, and if $\{a_1, a_2, \dots, a_m\}'$ be the negative symmetric group of the letters $a_1, a_2, \dots, a_m$, each letter referring to a different quantic, then

$$\{\mathrm{a}_1 \mathrm{a}_2 \dots \mathrm{a}_m\}' \Phi = \mid a_1 a_2 \dots a_m Q \mid,$$

where Q refers to the coefficients of a concomitant type of order m, viz., $(Q_0, Q_1, \dots, Q_m \between x_1, x_2)^m$. Hence, as Γ'_{a_1} is a negative symmetric group degree $a_1 = m$, in this case

$$T_{a_1, a_2, \dots, a_h} F = \Sigma \mid a_1 a_2 \dots a_m Q \mid .$$

And it follows that every rational integral concomitant of any number of m-ics can be expressed as a sum of terms each of which is a product of concomitants of types which give irreducible forms for $m-1$ m-ics, and of types of the form

$$| a_1 a_2 \dots a_m Q |,$$

where $(Q_0, Q_1, \dots, Q_m \between x_1, x_2)^m$ is a covariant type order m. If $| a_1, a_2, \dots, a_{m+1} |$ is reducible as in the case of the cubic, it follows at once that $| a_1 a_2 \dots a_m Q |$ is reducible; and hence that all types which give no irreducible form for $m-1$ m-ics are reducible.

Similar results follow for ternary forms, and, in fact, for forms with any number of variables. Thus, for types of the ternary m-ic, we suppose, as before, that each letter refers to one m-ic, and that the coefficients of the m-ic a_1 are

$$a_{1,1}\, a_{1,2} \dots a_{1,\frac{1}{2}(m+1)(m+2)}.$$

Thus we are dealing in reality with functions of n sets of variables, there being $\frac{1}{2}(m+1)(m+2)$ variables in each set. Every type which gives no irreducible concomitant for $\frac{1}{2}(m+1)(m+2)-1$ m-ics is reducible, with the single exception of the determinant of $\frac{1}{2}(m+1)(m+2)$ rows formed by the coefficients of this number of m-ics.

Moreover, the proof has nothing to do with the fact that the functions are invariant; except that none of the operations employed destroy the property of invariance. Similar results might be deduced for other kinds of algebraic functions.

Again, if $F=0$ be a syzygy between types of a binary m-ic, then every term of $\Gamma' F$ vanishes when Γ' is a negative symmetric group of degree greater than $m+1$. Hence, expanding F by the theorem of § 15, it follows that every syzygy between types must give at least one syzygy, when not more than $m+1$ m-ics are under discussion, which does not reduce to a mere identity; with the exception of syzygies which are wholly due to the fact that

$$\Gamma' Q = 0,$$

where Γ' is a negative symmetric group degree greater than $m+1$, and Q is any product of m-ic types. For, suppose that $F=0$ is a syzygy which always reduces to an identity when less than $m+2$ binary m-ics are under discussion; then, if $\alpha_1 < m+2$, each of the terms

$$T_{\alpha_1, \alpha_2, \dots, \alpha} F$$

is identically zero. Further, if $\alpha_1 > m+1$, each of the terms

$$T_{\alpha_1, \alpha_2, \dots, \alpha_h} F$$

is zero, being the sum of terms such as $\Gamma' Q$ mentioned above. Hence

F, which is $= \Sigma A_{a_1, \dots, a_k} \cdot T_{a_1, \dots, a_k} F$, is the sum of such terms, and $F = 0$ is a syzygy of that nature. As an example of a syzygy of this nature we have that between quadratic invariant types

$$[ab] = a_0 b_2 + a_2 b_0 - 2a_1 b_1,$$

viz., $$\{\mathrm{bdfh}\}' [ab][cd][ef][gh] = 0.$$

(3) To find the system of concomitants for r binary m-ics. Let F be any type, then, if Γ'_{r+1} be any negative symmetric group degree $r+1$, of the letters $a_1, a_2, \dots, a_n$,

$$\Gamma'_{r+1} F = 0,$$

for there are not more than r different quantics represented by the letters, so that amongst $r+1$ letters at least two must refer to some one quantic. This is necessary; it is also sufficient, for

$$F = \Sigma A_{a_1, \dots, a_k} \cdot T_{a_1, \dots, a_k} F,$$

and, if $a_1 > r_1$, $$T_{a_1, \dots, a_k} F = 0;$$

but, if a_1 is equal to or less than r, the term is obtainable by polarization from a concomitant of not more than r m-ics. Hence in this case we take the ordinary relations for the type F, coupled with all possible equations of the form

$$\Gamma'_{r+1} F = 0.$$

(4) The complete solution of the simultaneous system of equations

$$\Gamma'_{r+1} F = R,$$

where Γ'_{r+1} is any negative symmetric group of degree $r+1$, of the letters $a_1, a_2, \dots, a_n$, and there is one equation for every combination of these letters $r+1$ at a time, is

$$F = \Sigma G_1 G_2 \dots G_\nu f + R', \quad \nu < r+1,$$

where $G_1, G_2, \dots, G_\nu$ are positive symmetric groups no two of which have a common letter, but which between them contain all the n letters, and R' is a function obtained from the R's by means of substitutions alone. This is evidently a solution, for, provided that R' is chosen so that

$$\Gamma'_{r+1} R' = R,$$

it satisfies each of the equations. Moreover

$$F = \Sigma A_{a_1, a_2, \dots, a_k} \cdot T_{a_1, a_2, \dots, a_k} F,$$

and $T_{a_1, a_2, \ldots, a_h} F = R_1$, if $a_1 > r$, where R_1 is obtained in a definite manner from the given functions R, since $T_{a_1, a_2, \ldots, a_h} = \Sigma P.N$, where N contains as a factor a negative symmetric group degree a_1. And further, if $a_1 \leqslant r_1$,

$$T_{a_1, a_2, \ldots, a_h} = \Sigma PN,$$

where

$$P = G_1 G_2 \ldots G_\nu,$$

ν being $<r+1$, and the groups $G_1, G_2, \ldots, G_\nu$ having the character laid down above. The solution is then the complete one, and we see further that, in each term of the sum $\Sigma G_1 G_2 \ldots G_\nu f$, f is such that it may be obtained from F by means of the operation of the product N of certain definite negative symmetric groups.

Conversely, the complete solution of all possible equations of the form

$$G_1 G_2 \ldots G_\nu F = R, \quad \nu < r+1,$$

where the groups $G_1, G_2, \ldots, G_\nu$ are positive symmetric groups, no two of which contain a common letter, and which between them contain all the letters $a_1, a_2, \ldots, a_n$, is

$$F = \Sigma \Gamma'_{r+1} f + R',$$

where Γ'_{r+1} is a negative symmetric group degree $r+1$, and R' a function obtained from the R's by means of substitutions alone; and, further, the f for each term may be obtained from F by means of substitutions alone.

(5) In exactly the same way it may be shown that, if G_{r+1} is a positive symmetric group degree $r+1$, the solution of all possible equations of the form

$$G_{r+1} F = R$$

is

$$F = \Sigma \Gamma'_1 \Gamma'_2 \ldots \Gamma'_\nu f + R', \quad \nu < r+1.$$

(6) Suppose that G_r is the alternating group of certain r letters, that $G_r^{(1)}$ is the positive symmetric group of the same letters, and that $G_r^{(2)}$ is the negative symmetric group. Then, if

$$G_r F = 0,$$

it follows that

$$G_r^{(1)} F = 0 \quad \text{and} \quad G_r^{(2)} F = 0.$$

For, if a and b are any two letters affected by G_r, then

$$G_r^{(1)} = \left[1 + (\mathrm{ab})\right] G_r$$

and

$$G_r^{(2)} = \left[1 - (\mathrm{ab})\right] G_r.$$

Consider, then, the simultaneous system of equations

$$G_r F = 0,$$

where the r letters affected by G_r are chosen in any manner from the letters $a_1, a_2, \ldots, a_n$, there being one equation for each combination of these letters r at a time; then

$$F = \Sigma A_{a_1, a_2, \ldots, a_h} \cdot T_{a_1, a_2, \ldots, a_h} F,$$

and all terms of this expansion vanish in which T possesses either positive or negative symmetric groups of degree $\geqslant r$. Hence, if

$$T_{a_1, a_2, \ldots, a_h} F$$

is not zero, $a_1 < r$ and $h < r$; for a_1 is the degree of the greatest negative symmetric group, and h that of the greatest positive symmetric group contained in T. Now

$$a_1 \nless a_2 \nless a_3 \nless \ldots \nless a_h;$$

and hence $$n = a_1 + a_2 + \ldots + a_h \ngtr h a_1;$$

and therefore, in order that both h and a_1 may be $< r$, we must have

$$n \ngtr (r-1).$$

If therefore $n > (r-1)^2$, every term

$$T_{a_1, a_2, \ldots, a_h} F$$

is zero, and F itself is zero.

On Group-Characteristics. *By* W. Burnside.

Received and communicated November 8th, 1900.

In a series of memoirs published in the *Berliner Sitzungsberichte* ("Über Gruppencharaktere," 1896, pp. 985–1021; "Über die Primfactoren der Gruppendeterminante," 1896, pp. 1343–1382; and others) Herr Frobenius has developed a theory of group-characteristics which must have a far-reaching importance in connexion with groups of finite order. For Abelian groups, an admirable account of the theory will be found in the second volume of Herr Weber's *Lehrbuch der Algebra.* The extension of the theory to non-

Abelian groups, is, however, quite a new departure. The present paper has been written with the intention of introducing this new development in the theory of groups of finite order to English readers. It is not original, as the results arrived at are, with one or two slight exceptions, due to Herr Frobenius. The modes of proof, however, are, in general, quite distinct from those used by Herr Frobenius. It will facilitate the reading of the paper to state what a group-characteristic, or, rather, a set of group-characteristics, actually is; though this statement is not, in fact, taken as the starting-point of the theory.

A group of finite order g is said to be *represented* as an *irreducible* group of linear substitutions on m variables when g is simply or multiply isomorphic with the group of linear substitutions, and when it is impossible to choose m' $(<m)$ linear functions of the variables which are transformed among themselves by every operation of the group. Any two conjugate operations of the group when brought to canonical form have the same multipliers. The sum of these multipliers is called the *characteristic* of the set of conjugate operations, or of any one of them, for the mode of representing the group in question; and the characteristics of the different sets of conjugate operations for one and the same mode of representation are called a *set* of characteristics. If g is multiply isomorphic with the group of linear substitutions, every operation of the self-conjugate sub-group of g which corresponds to the identical operation of the group of linear substitutions has m (the number of variables) for its characteristic. In particular every group is multiply isomorphic with the group

$$x' = x,$$

constituted by the identical operation only; so that among the sets of characteristics of any group there is always one set in which each characteristic is unity.

1. Let
$$S_1 (= 1),\ S_2,\ \ldots,\ S_n$$
be the operations of a group g of finite order n. Also let r be the number of distinct conjugate sets of operations contained in the group, and $h_1 (= 1)$, h_2, ..., h_r the number of operations in each set, so that
$$n = h_1 + h_2 + \ldots + h_r.$$
The first set consists of the identical operation only. Represent by C_i the totality of the operations of the i-th conjugate set, each operation taken once. The product
$$C_i C_j$$

consists of h_ih_j operations of g, which are not in general all distinct. Since

$$S^{-1}C_iC_jS = C_iC_j,$$

whatever operation S may be of g, the h_ih_j operations of C_iC_j can be divided into a number of conjugate sets. Hence we may write

$$C_iC_j = \sum_{s=1}^{s=r} c_{ijs}C_s, \tag{1}$$

where each coefficient c_{ijs} is a positive integer or zero.

If R_j is any operation of C_j, then

$$R_j^{-1}C_iR_j = C_i$$

or
$$C_iR_j = R_jC_i.$$

Hence
$$C_iC_j = C_jC_i$$

and
$$c_{ijs} = c_{jis}.$$

Again, the product $C_iC_jC_k$ is shewn in a similar manner to be independent of the sequence of its factors. But

$$C_iC_jC_k = \sum_s c_{ijs}C_sC_k = \sum_{s,t} c_{ijs}c_{skt}C_t.$$

Hence, for each t, the symbol $\sum_s c_{ijs}c_{skt}$ is independent of permutations of i, j, and k. If C_iR_j contains ν operations of the s-th set, so also does $C_iR'_j$, where R'_j is any other operation of the j-th set. Hence the number of operations of the s-th set in C_iC_j is a multiple of h_j and also of h_i. This number, however, is $c_{ijs}h_s$; so that $c_{ijs}h_s$ is equal to or is a multiple of the L.C.M. of h_i and h_j. The equation

$$h_ih_j = \sum_s c_{ijs}h_s$$

expresses that the number of operations on either side of equation (1) is the same. If

$$R_1, R_2, \ldots, R_{h_i}$$

are the operations of the i-th set, then

$$R_1^{-1}, R_2^{-1}, \ldots, R_{h_i}^{-1}$$

constitute a conjugate set. This is called the *inverse* set of the previous one. These two sets may be identical, in which case the i-th set is called a *self-inverse* set. In any case the index of the inverse set of the i-th set will be represented by i'; so that the i-th and i'-th sets are inverse, while i and i' are the same for a self-inverse set. The number of operations in two inverse sets is obviously the same; so that

$$h_i = h_{i'}.$$

With this notation, it follows at once from the definition of c_{ijs} that

$$c_{ijs} = c_{i'j's'}$$

and $$c_{ijs} h_s = c_{is'j'} h_j.$$

A group of even order necessarily has self-inverse conjugate sets, in addition to that constituted by the identical operation alone, since an operation of order 2 is the same as its inverse.

2. Let $$x = \Sigma x_t S_t, \quad x' = \Sigma x'_t S_t, \quad x'' = \Sigma x''_t S_t,$$

where x_t, x'_t, x''_t are variables, and the symbols S_t are subject only to the multiplication table of the group g. The product $x'x$ is another definite expression of the same form as x or x'. If this is x'', then

$$x''_t = \Sigma x'_j x_i,$$

where the summation is extended to all suffixes such that

$$S_t = S_j S_i.$$

Hence, if the suffixes of the x's combine according to the same laws as the operations of g, so that

$$y_{pq} = y_s,$$

when $$S_p S_q = S_s,$$

then $$x''_t = \Sigma x'_{ti^{-1}} x_i \quad (t = 1, 2, \ldots, n)$$

are the conditions that x'' should equal $x'x$. These are the finite equations of the continuous group G, considered in § 2 of my second paper "On the Continuous Group defined by any given Group of Finite Order" (*Proc. Lond. Math. Soc.*, Vol. XXIX., pp. 555 *et seq.*). It is there shewn that the sub-group H, constituted of the self-conjugate operations of G, arises by making

$$x'_p = x'_q,$$

if S_p and S_q are conjugate operations of g; and that, if

$$x'_p = \epsilon_s,$$

when S_p belongs to the s-th conjugate set of g, then the characteristic determinant of H is of the form

$$\prod_{i=1}^{i=r} (\lambda + \epsilon_1 + a_{i2}\epsilon_2 + \ldots + a_{ir}\epsilon_r)^{\mu_i^2},$$

where the r expressions

$$\epsilon_1 + a_{i2}\epsilon_2 + \ldots + a_{ir}\epsilon_r \quad (i = 1, 2, \ldots, r)$$

or, in other words, the r multipliers of H, are linearly independent.

The parameter group of H will be the linear homogeneous group in r variables which results by making

$$x_p = x_q, \quad x'_p = x'_q, \quad x''_p = x''_q,$$

when S_p and S_q are conjugate operations of g. With this limitation, x, x', x'' become ϵ, ϵ', ϵ'', where

$$\epsilon = \Sigma \epsilon_t C_t, \quad \epsilon' = \Sigma \epsilon'_t C_t, \quad \epsilon'' = \Sigma \epsilon''_t C_t$$

and $$\epsilon'' = \epsilon'\epsilon = \epsilon\epsilon',$$

if $$\sum_t \epsilon''_t C_t = \sum_{p,q} \epsilon'_p \epsilon_q C_p C_q = \sum_{p,q,t} c_{pqt} \epsilon'_p \epsilon_q C_t$$

or if $$\epsilon''_t = \sum_{p,q} \epsilon'_p \epsilon_q c_{pqt} \quad (t = 1, 2, \dots, r).$$

The linear homogeneous group in r variables given by these equations has therefore the r linearly independent invariants

$$\epsilon_1 + a_{i2}\epsilon_2 + \dots + a_{ir}\epsilon_r \quad (i = 1, 2, \dots, r).$$

I introduce now the notation used by Herr Frobenius, and write*

$$\mu_i = \chi^i_1, \quad a_{is} = \frac{h_s \chi^i_s}{\chi^i_1}:$$

so that the invariants of the group of the ϵ's are

$$\Sigma h_s \chi^i_s \epsilon_s \quad (i = 1, 2, \dots, r).$$

The r quantities $$\chi^i_1, \chi^i_2, \dots, \chi^i_r$$

are called by Herr Frobenius a set of group-characteristics (*Gruppencharaktere*), and there are r such sets corresponding to the r values of the upper index.

The infinitesimal operators of the group of the ϵ's are

$$E_j = \sum_{i,s} c_{ijs} \epsilon_i \frac{\partial}{\partial \epsilon_s} \quad (j = 1, 2, \dots, r);$$

and, if I is any invariant of the group, then

$$E_j I = \kappa_j I,$$

where κ_j is a constant.

Dropping now for a moment the upper suffix and representing by

$$\chi_1, \chi_2, \dots, \chi_r$$

any set of group-characteristics, $\Sigma h_s \chi_s \epsilon_s$ is an invariant of the group.

---

* The i in χ^i_s is not an index, but is used to avoid a double suffix.

But
$$E_j \sum_s h_s \chi_s e_s = \sum_{i,s} c_{ijs} h_s \chi_s e_i = \kappa_j \sum_s h_s \chi_s e_s,$$

and, therefore, comparing the coefficients of e_1,

$$\kappa_j \chi_1 = \sum_s c_{1js} h_s \chi_s.$$

Now, from its definition, c_{1js} is zero, unless $s=j$, and c_{1jj} is unity. Hence

$$\kappa_j \chi_1 = h_j \chi_j,$$

so that
$$h_j \chi_j \sum_s h_s \chi_s e_s = \chi_1 \sum_{i,s} c_{ijs} h_s \chi_s e_i;$$

and, therefore, equating coefficients of e_k,

$$h_j h_k \chi_j^i \chi_k^i = \chi_1^i \sum_s c_{jks} h_s \chi_s^i \tag{1}$$

is true for all values of j, k, and i. These equations are homogeneous in the χ's, and the coefficients are integers depending on the multiplication table of the group. Moreover, if for a moment we write

$$\frac{h_j \chi_j^i}{\chi_1^i} = \lambda_j,$$

the form of the equations is

$$\lambda_j \lambda_k = \sum c_{jks} \lambda_s,$$

which is identical with that of equations (i) of § 1 giving the product of the conjugate sets. It is then an immediate consequence of what has been proved that, if in equations (i) of § 1 the C's be regarded as symbols of quantity, the equations admit exactly r sets of solutions,[*] and that these solutions are linearly independent. Consider now the infinitesimal operation $\sum_j \chi_{j'}^i E_j$. We have

$$\begin{aligned}\sum_j \chi_{j'}^i E_j &= \sum_{j,k,s} c_{kjs} \chi_{j'}^i e_k \frac{\partial}{\partial e_s} \\ &= \sum_{j,k,s} \frac{c_{ks'j'} h_j}{h_s} \chi_{j'}^i e_k \frac{\partial}{\partial e_s} \\ &= \sum_{k,s} \frac{h_k \chi_k^i \chi_{s'}^i}{\chi_1^i} e_k \frac{\partial}{\partial e_s} \\ &= \frac{1}{\chi_1^i} \sum_k h_k \chi_k^i e_k \sum_s \chi_{s'}^i \frac{\partial}{\partial e_s}.\end{aligned}$$

This operator, therefore, either annihilates a linear function of the e's, or changes it into a multiple of $\sum h_k \chi_k^i e_k$.

---

[*] In fact, if there were more than r solutions, H would have more than r invariants.

Hence, if j is different from i,

$$\sum_s \chi^i_{s'} \frac{\partial}{\partial \epsilon_s} \sum_s h_s \chi^j_s \epsilon_s = 0,$$

or

$$\sum_s h_s \chi^j_s \chi^i_{s'} = 0 \quad (i \neq j). \tag{ii}$$

Since the r invariants are linearly independent, the determinant

$$\begin{vmatrix} \chi^1_1, & \chi^1_2, & \dots, & \chi^1_r \\ \chi^2_1, & \chi^2_2, & \dots, & \chi^2_r \\ \dots & \dots & \dots & \\ \chi^r_1, & \chi^r_2, & \dots, & \chi^r_r \end{vmatrix}$$

of the χ's is not zero. Hence, from the equations (ii), it follows that the r quantities

$$h_s \chi^i_{s'} \quad (s = 1, 2, \dots, r)$$

are proportional to the minors of the r terms

$$\chi^i_s \quad (s = 1, 2, \dots, r)$$

in the i-th line of the determinant. If the ratio is γ_i, so that

$$\gamma_i h_s \chi^i_{s'} = X^i_s,$$

where X^i_s is the minor of χ^i_s in X, the determinant of the χ's, then

$$X = \gamma_1 \chi^1_1 \chi^1_1 + \gamma_2 \chi^2_1 \chi^2_1 + \dots + \gamma_r \chi^r_1 \chi^r_1,$$
$$0 = \gamma_1 \chi^1_1 \chi^1_2 + \gamma_2 \chi^2_1 \chi^2_2 + \dots + \gamma_r \chi^r_1 \chi^r_2,$$
$$\dots \quad \dots \quad \dots \quad \dots \quad \dots$$
$$0 = \gamma_1 \chi^1_1 \chi^1_r + \gamma_2 \chi^2_1 \chi^2_r + \dots + \gamma_r \chi^r_1 \chi^r_r.$$

Another similar set of equations is obtained by considering the characteristic determinant of G. In the undeveloped form (*loc. cit.*, p. 556) each term in the leading diagonal is $\lambda + \epsilon_1$; so that when expanded in descending powers of λ it has the form

$$\lambda^n + n\epsilon_1 \lambda^{n-1} + \text{terms in } \lambda^{n-2}, \text{ \&c.}$$

On the other hand, the characteristic determinant is

$$\prod_1^r \left(\lambda + \frac{1}{\chi_1} \sum_s h_s \chi^i_s \epsilon_s \right)^{(\chi^i_1)^2} = \lambda^n + \lambda^{n-1} \sum_{s,\,i} \epsilon_s \chi^i_1 \chi^i_s + \dots.$$

Hence

$$n = \chi^1_1 \chi^1_1 + \chi^2_1 \chi^2_1 + \dots + \chi^r_1 \chi^r_1,$$
$$0 = \chi^1_1 \chi^1_2 + \chi^2_1 \chi^2_2 + \dots + \chi^r_1 \chi^r_2,$$
$$\dots \quad \dots \quad \dots \quad \dots$$
$$0 = \chi^1_1 \chi^1_r + \chi^2_1 \chi^2_r + \dots + \chi^r_1 \chi^r_r.$$

Comparing these equations with the preceding set, it follows that

$$\gamma_1 = \gamma_2 = \ldots = \gamma_r = \frac{X}{n}$$

and that the minor of χ^i_s in X is

$$\frac{h_s}{n} X \chi^i_{s'}.$$

The determinant whose elements are the first minors of X is X^{r-1}; and therefore

$$X^2 = (-1)^k \frac{n^r}{\prod\limits_1^r h_s},$$

where k is the number of pairs of inverse sets.

Since $\frac{h_s}{n} X \chi^i_{s'}$ is the minor of χ^i_s in the determinant of the χ's, the following systems of relations hold among the group-characteristics, viz.,

$$\sum_{k=1}^{k=r} h_k \chi^i_k \chi^i_{k'} = n, \tag{iii}$$

$$\sum_{k=1}^{k=r} h_k \chi^i_k \chi^j_{k'} = 0 \quad (i \neq j), \tag{iv}$$

$$\sum_{i=1}^{i=r} \chi^i_k \chi^i_{k'} = \frac{n}{h_k}, \tag{v}$$

$$\sum_{i=1}^{i=r} \chi^i_k \chi^i_l = 0 \quad (l \neq k'). \tag{vi}$$

These relations are capable of being presented in a slightly different form. Among the invariants of the group of the ϵ's the function $\Sigma h_s \chi^i_{s'} \epsilon_s$ must occur. In fact,

$$\begin{aligned} E_j \,.\, \Sigma h_s \chi^i_{s'} \epsilon_s &= \sum_{t,s} c_{tjs} h_s \chi^i_{s'} e_t \\ &= \sum_{t',s'} c_{t'j's'} h_{s'} \chi^i_{s'} e_t \\ &= \sum_{t'} \frac{h_{t'} h_{j'} \chi^i_{t'} \chi^i_{j'}}{\chi^i_1} e_t \\ &= \frac{h_{j'} \chi^i_{j'}}{\chi^i_1} \Sigma_t h_t \chi^i_{t'} e_t. \end{aligned}$$

Hence there must be a set of characteristics

$$\chi^j_1,\ \chi^j_2,\ \ldots,\ \chi^j_s,\ \ldots,\ \chi^j_r,$$

which are proportional, term for term, to

$$\chi_{1'}^{i},\ \chi_{2'}^{i},\ \ldots,\ \chi_{s'}^{i},\ \ldots,\ \chi_{r'}^{j};$$

and, since
$$n = \sum_k h_k \chi_k^j \chi_{k'}^j = \sum_k h_k \chi_{k'}^i \chi_k^i,$$

the two sets must be equal term for term. If

$$\chi_s^i = \chi_{s'}^i$$

for each s, the two sets are the same. Such a set is called a *self-inverse* set. If, however, the relation

$$\chi_s^i = \chi_{s'}^i$$

does not hold for all suffixes s, the two sets of characteristics are distinct. They are called *inverse* sets, and will always be represented by upper suffixes i and i'; so that

$$\chi_s^i = \chi_{s'}^{i'}$$

and
$$\chi_{s'}^i = \chi_s^{i'}.$$

With this notation, equations (iii)—(vi) may be written in the alternative forms :—

$$\sum_{k=1}^{k=r} h_k \chi_k^i \chi_k^{i'} = n, \qquad \text{(iii)}'$$

$$\sum_{k=1}^{k=r} h_k \chi_k^i \chi_k^j = 0 \quad (j \neq i'), \qquad \text{(iv)}'$$

$$\sum_{i=1}^{i=r} \chi_k^i \chi_k^{i'} = \frac{n}{h_k}, \qquad \text{(v)}'$$

$$\sum_{i=1}^{i=r} \chi_k^i \chi_l^{i'} = 0 \quad (l \neq k). \qquad \text{(vi)}'$$

3. Returning now to the continuous group G, it is shown (*loc. cit.*, p. 560) that its characteristic determinant D is expressible in the form

$$\prod_{i=1}^{i=r} P_i^{\chi_1^i},$$

where P_i is an irreducible homogeneous function of $\lambda + y_1, y_2, \ldots, y_n$ of degree χ_1^i; and that to each irreducible factor P_i of D there corresponds an irreducible component of G in χ_1^i variables of which P_i is the characteristic determinant. Moreover, the n operations of this irreducible component of G, given by

$$y_1 = y_2 = \dots = y_{s-1} = y_{s+1} = \dots = y_n = 0, \quad y_s = 1$$
$$(s = 1, 2, \dots, n),$$

constitute an irreducible group γ of finite order in the χ_1 variables, with which g is simply or multiply isomorphic. The leading term in P_i written in descending powers of $\lambda + y_1$ is $(\lambda + y_1)^{\chi_1^i}$, and we may write

$$P_i = (\lambda + y_1)^{\chi_1^i} + (\lambda + y_1)^{\chi_1^i - 1} \sum_{s=2}^{s=r} b_s y_s + \dots.$$

The characteristic equation of the operation of γ which corresponds to

$$y_1 = \dots = y_{s-1} = y_{s+1} = \dots = y_n = 0, \quad y_s = 1$$

is therefore $$0 = \lambda^{\chi_1^i} + b_s \lambda^{\chi_1^i - 1} + \dots,$$

and hence b_s is the sum of the multipliers of this operation. Now two conjugate operations have necessarily the same multipliers. Hence, if S_p and S_q are conjugate operations of g, then

$$b_p = b_q.$$

If, now, in P_i, y_p is replaced by ϵ_t when S_p belongs to the t-th conjugate set in g, then (*loc. cit.*, p. 561) P_i becomes

$$\left(\lambda + \frac{1}{\chi_1^i} \sum_{s=1}^{s=r} h_s \chi_s^i \epsilon_s\right)^{\chi_1^i}.$$

On the other hand, P_i may then be written

$$\lambda^{\chi_1^i} + \lambda^{\chi_1^i - 1} (\chi_1^i \epsilon_1 + \sum_{t=2}^{t=r} b_t h_t \epsilon_t) + \dots,$$

where b_t is the common value of the b's which occur in connexion with these y's that correspond to operations of the t-th conjugate set. Comparing these two expressions for P_i, it follows that χ_s^i is the sum of the multipliers of any one of the s-th set of conjugate operations of g, when represented as an irreducible group in χ_1^i variables of the form under consideration. Hence, if m is the order of the operations of the s-th set, then χ_s^i is the sum of χ_1^i m-th roots of unity.

Moreover, the r sets of characteristics give the sums of the multipliers of the operations of g for the r distinct irreducible groups that correspond to the r distinct irreducible factors of D; and (*loc. cit.*, p. 565), conversely, the sums of the multipliers of any irreducible representation of g are given by one of the sets of characteristics.

To the factor $\lambda+y_1+y_2+\dots+y_n$

of D there corresponds the set of characteristics each of which is unity. This will be taken as

$$\chi^1_1,\ \chi^1_2,\ \dots,\ \chi^1_r.$$

If $\omega, \omega', \omega'', \dots$ are the multipliers of S in any representation of the group, then $\omega^{-1}, \omega'^{-1}, \omega''^{-1}, \dots$ are the multipliers of S^{-1}. Hence χ^i_s and $\chi^i_{s'}$ are either real and equal, or they are conjugate imaginaries. Each of the members of a self-inverse set of characteristics is therefore real, while corresponding members of two inverse sets are either real and equal or are conjugate imaginaries.

Every group-characteristic, being a sum of roots of unity, is an algebraic integer, while the χ_1's are real positive integers. Now equation (i) of § 2 becomes in a particular case

$$h^2_k\chi^i_k\chi^i_{k'} = \chi^i_1\sum_s c_{kk's}h_s\chi^i_s$$

$$= \chi^i_1\sum_s c_{s'kk}h_k\chi^i_s$$

or

$$h_k\chi^i_k\chi^i_{k'} = \chi^i_1\sum_s c_{s'kk}\chi^i_s;$$

and, summing each side with respect to k,

$$n = \chi_1\sum_{s,k} c_{s'kk}\chi^i_s.$$

Hence $\frac{n}{\chi^i_1}$ is an algebraic integer, and, being a rational number, it must be a real integer. If, then, a group of order n can be represented as an irreducible group of linear substitutions in m variables, m must be a factor of n.

From equation (i) of § 2 an equation may be derived whose roots are the r values of $(\chi^i_1)^2$. Thus

$$h_ph_q\chi^i_p\chi^i_q = \chi^i_1\sum_s c_{pqs}h_s\chi^i_s$$

gives

$$h_p\chi^i_p.h_q\chi^i_q\chi^i_{q'} = \chi^i_1\sum_s c_{pqs}h_s\chi^i_s\chi^i_{q'},$$

$$= (\chi^i_1)^2\sum_s c_{pqs}\sum_t\frac{c_{sq't}h_t}{h_q}\chi^i_t,$$

$$= (\chi^i_1)^2\sum_{s,t} c_{pqs}c_{st'q}\chi^i_t.$$

Therefore, summing with respect to q,

$$h_p\chi^i_pn = (\chi^i_1)^2\sum_{s,t,q} c_{pqs}c_{st'q}\chi^i_t.$$

There are r distinct equations of this form, corresponding to the r values of p, whatever i may be. Hence, on eliminating the ratios of $\chi_1^i, \chi_2^i, \ldots, \chi_r^i$, an equation of the r-th degree for $(\chi_1^i)^2$ results.

4. The characteristics of a group may often be classified in sets more extensive than those given by pairing inverse sets. Each of the r characteristics of a set being a sum of roots of unity, there must exist, unless the characteristics are all rational, and therefore integral, some algebraic integer a satisfying an irreducible equation with rational coefficients, in terms of which each of the characteristics of a set can be rationally expressed. If P is the irreducible factor of the determinant D, which corresponds to the set of characteristics, some at least of the coefficients in P are rational functions of a. Now the coefficients in D are rational integers. Hence, if P becomes P' when a is replaced by any other root a' of the irreducible equation which it satisfies, P' must be a factor of D. This is equivalent to the statement that, if

$$\chi_1, \chi_2, \ldots, \chi_r$$

become

$$\chi_1', \chi_2', \ldots, \chi_r',$$

when a is replaced by a', then this latter set of quantities is a set of group-characteristics. The number of sets of characteristics in such a system is clearly equal to, or is a factor of, the degree of the equation satisfied by a.*

The considerations thus applied to a set of characteristics may also be used in connexion with the coefficients of the individual substitutions of any group of linear substitutions of finite order. In the most general case these can be expressed as rational functions of some algebraic integer a, satisfying an irreducible equation with rational coefficients, and of a finite number of arbitrary constants.† If A, B, C are any three substitutions of the group, such that

$$AB = C,$$

and, if A', B', and C' are the three substitutions that arise on replacing

---

* In fact, a is a cyclotomic function, and therefore the order of the group of the equation it satisfies is equal to its degree.

† That such constants may occur will be evident from a simple instance. Thus the group generated by

$$x' = \omega x, \quad y' = \omega^2 y, \quad z' = \omega^4 z, \quad \text{and} \quad x' = \alpha y, \quad y' = \beta z, \quad z' = \frac{1}{\alpha\beta} x,$$

where $\omega^7 = 1$ is a group of order 21.

a by a', any other root of the equation for a, then, because the equation is irreducible,

$$A'B' = C'.$$

Hence, the original group and the new group that arises on replacing a by a' in all the coefficients are simply isomorphic in such a way that A and A' are corresponding operations.

Suppose, in particular, that the group is an irreducible group expressed in such a form that one of its substitutions of S of order m is in canonical form. If ω is a primitive m-th root of unity, the coefficients in S are powers of ω. Hence, if ω is replaced by any other primitive m-th root ω' in all the substitutions, the group is represented as simply isomorphic with itself. If in the original form

$$\omega^a,\ \omega^b,\ \ldots$$

are the multipliers of S, then, in the new form

$$\omega'^a,\ \omega'^b,\ \ldots$$

are its multipliers. Unless the m-th roots contained in these two series are the same, the second form of the group cannot be the result of transforming the first form; so that the characteristic

$$\chi' = \omega'^a + \omega'^b + \ldots$$

belongs to a distinct set of characteristics from

$$\chi = \omega^a + \omega^b + \ldots$$

though in particular cases χ and χ' may be equal to each other. For instance, if S is a substitution of order 9, and if, ω being a primitive ninth root of unity, the group has a set of characteristics for which χ_1 is 3 and the characteristic of S is

$$\chi = \omega + \omega^4 + \omega^7 = 0,$$

then the group must have a second set of characteristics in which χ_1' is 3 and the characteristic of S is

$$\chi' = \omega^2 + \omega^8 + \omega^5 = 0.$$

If S is an operation of order m, and if S and S^r are conjugate operations, then in every representation of the group the characteristics of S and S^r are the same. Hence, if ω is a primitive m-th root of unity, and χ is any characteristic of S, χ must be unaltered when ω^r is written for ω in each of the roots of unity whose sum is χ.

Conversely, if each of the characteristics of an operation S is unaltered when in it ω^r is written for ω, m being the order of S and ω

being a primitive m-th root of unity, then S and S^μ must be conjugate operations. For suppose, if possible, that they were not so; then in each set of characteristics those of S and S^μ are the same, and therefore those of S and $S^{-\mu}$ are either equal or they are conjugate imaginaries. Moreover, since S and S^μ do not belong to the same conjugate set, no more do S^{-1} and $S^{-\mu}$; so that S and $S^{-\mu}$ do not belong to inverse sets. If they belong to the k-th and l-th sets, then, since $k \neq l'$,

$$\sum_i \chi_k^i \chi_l^i = 0.$$

But, since χ_k^i and χ_l^i are conjugate imaginaries, this is impossible. The supposition that S and S^μ are not conjugate leads therefore to a contradiction. In particular, for a group of odd order, all the characteristics

$$\chi_k^1, \chi_k^2, \ldots, \chi_k^r$$

of the same conjugate set of operations cannot be real. For, if they were, S and S^{-1} would be conjugate operations, S being any operation of the set.

5. I consider now the relations between the characteristics of a group g and those of a group g', with which g is multiply isomorphic. If g is simple, every irreducible representation of g, except that given by the first set of characteristics, is simply isomorphic with g. If g has a self-conjugate sub-group h, and if the factor-group g/h is simply isomorphic with g', I have shewn (*loc. cit.*, pp. 563, 564) how to construct, corresponding to any irreducible factor P' of the determinant of g', an irreducible factor P of the same degree of the determinant of g. If T_i' is any operation of g', and

$$T_i,\ T_iS_2,\ T_iS_3,\ \ldots,\ T_iS_\mu$$

the corresponding operations of g, the process consists in replacing in P' the y that corresponds to T_i' by the sum of the y's which correspond to $T_i, T_iS_2, \ldots, T_iS_\mu$. In the set of characteristics of g which correspond to this irreducible factor P each operation of h has the same characteristic as the identical operation; and any two operations S and S' of g which are such that SS'^{-1} belongs to h have the same characteristic.

If g' is Abelian, the irreducible factors of its determinant are all linear, and so also are the corresponding irreducible factors of the determinant of g. Conversely, if the determinant of g has a linear factor other than the first, g is multiply isomorphic with a cyclical group. Hence the necessary and sufficient condition that g shall have a set of characteristics other than the first, for which χ_1^i is unity, is that g has a self-conjugate sub-group h, for which g/h is Abelian, or, in other words, that g shall not be a perfect group. Moreover, the number of such sets, including the first, is the ratio of the order of g to the order of its derived group; for this is the order of the greatest Abelian group with which g is multiply isomorphic.

6. Let
$$x_s' = \Sigma a_{stm} x_t,$$
$$(s, t = 1, 2, \ldots, \chi_1^i),$$
$$(m = 1, 2, \ldots, n),$$
be an irreducible representation of the group g with characteristics
$$\chi_1^i,\ \chi_2^i,\ \ldots,\ \chi_r^i;$$
and
$$y_s' = \Sigma \beta_{stm} y_t,$$
$$(s, t = 1, 2, \ldots, \chi_1),$$
$$(m = 1, 2, \ldots, n),$$
another irreducible representation of the group with characteristics
$$\chi_1^j,\ \chi_2^j,\ \ldots,\ \chi_r^j.$$

Then the $\chi_1^i \chi_1^j$ products $x_s y_t$ are transformed linearly among themselves by every operation of the group. In the representation of g thus arrived at, the sum of the multipliers of any operation of the k-th conjugate set is $\chi_k^i \chi_k^j$. This is seen at once by supposing the group of the x's and the group of the y's so transformed that the operation in question appears in canonical form. Let the $\chi_1^i \chi_1^j$ $(= \mu)$ products be represented by $z_1, z_2, \ldots, z_\mu$; so that the z's are transformed by a group
$$z_s' = \Sigma \gamma_{stm} z_t,$$
$$(s, t = 1, 2, \ldots, \mu),$$
$$(m = 1, 2, \ldots, n).$$

The determinant
$$\Delta = \Big| \sum_m \gamma_{stm} u_m \Big|$$
of this group must (*loc. cit.*, p. 564) be the product of irreducible

factors of the original group determinant of g; so that we may write

$$\Delta = \prod_{s=1}^{s=r} P_s^{d_{ijs}},$$

where each index d_{ijs} is either zero or a positive integer. Hence, equating coefficients of $u_1^{n-1}u_k$ on either side of this equation,

$$\chi_k^i \chi_k^j = \sum_{s=1}^{s=r} d_{ijs} \chi_k^s, \tag{i}$$

$$(k = 1, 2, \ldots, r).$$

This system of equations among the group-characteristics is analogous to that given by equation (i) of § 2, where, however, the sign of summation applies to the lower index. If either side of equation (i) is multiplied by $h_k \chi_k^{s'}$, and the sum taken for all conjugate sets, it follows that, since

$$\sum_k h_k \chi_k^s \chi_k^{s'} = n,$$

and

$$\sum_k h_k \chi_k^s \chi_k^t = 0 \quad (t \neq s'),$$

$$nd_{ijs} = \sum_k h_k \chi_k^i \chi_k^j \chi_k^{s'}$$

$$= \sum_{k'} h_{k'} \chi_{k'}^i \chi_{k'}^j \chi_{k'}^{s'} = \sum_k h_k \chi_k^{i'} \chi_k^{j'} \chi_k^s.$$

Hence

$$d_{ijs} = d_{jis} = d_{is'j'} = d_{i'j's'}.$$

It is clear, from the definition of d_{ijs}, that

$$d_{i1i} = 1,$$

and

$$d_{i1j} = 0 \quad (j \neq i),$$

the first set of characteristics being that in which each characteristic is unity. Hence

$$d_{ii'1} = 1,$$

and

$$d_{ij1} = 0 \quad (j \neq i').$$

If the group has a set of characteristics, say the k-th, other than the first, for which χ_1^k is unity, then of the integers d_{iks} $(s = 1, 2, \ldots, r)$ one must be unity and the rest zero In fact,

$$d_{iks} \chi_1^s \leqslant \chi_1^i$$

and

$$d_{ks'i'} \chi_1^i \leqslant \chi_1^s;$$

so that d_{iks} is zero, unless $\chi_1^i = \chi_1^s$. Hence, if

$$\chi_1^i, \chi_2^i, \ldots, \chi_r^i$$

is any set of characteristics, and

$$\chi_1^k,\ \chi_2^k,\ \dots,\ \chi_r^k$$

a set for which χ_1^k is unity, then

$$\chi_1^k\chi_1^i,\ \chi_2^k\chi_2^i,\ \dots,\ \chi_r^k\chi_r^i$$

is a set of characteristics.

Returning to the irreducible representation of the group in the form

$$x_s' = \Sigma a_{stm} x_t,$$

the $\frac{1}{2}\chi_1^i(\chi_1^i+1)$ homogeneous products of the second degree of the x's are transformed linearly among themselves by every operation of the group; and, for this representation, the sum of the multipliers of any operation is equal to the sum of the homogeneous products two together of the multipliers in the above irreducible form. Hence, by similar reasoning to that employed above, there must be positive integers e_{is}, such that

$$\psi_k^i = \sum_s e_{is}\chi_k^s \quad (k,\ i = 1,\ 2,\ \dots,\ r), \qquad \text{(ii)}$$

where ψ_k^i is the sum of the homogeneous products two together of the multipliers whose sum is χ_k^i. In this way it may be shown that, if any symmetric function be formed of χ_1^i symbols, a system of equations of the form (ii), in which the e's are positive integers, must hold when ψ_k^i is the symmetric function formed from the multipliers whose sum is χ_k^i. In particular, the products of the multipliers for each set of conjugate operations in any representation of the group constitutes a set of characteristics for which χ_1 is unity.

On some Properties of Groups of Odd Order. By W. BURNSIDE.

Received and communicated November 8th, 1900.

This paper consists mainly of applications of the theory of group-characteristics given in the preceding paper to groups of odd order. It is shewn in the first section that a group of odd order has no self-inverse set of characteristics. From this it follows at once that such a group when represented as an irreducible group of linear substitutions must contain substitutions whose coefficients are not all real. In other words, a group of linear substitutions of odd order the coefficients in which are all real is necessarily reducible. Another consequence is that the order of such a group and the number of sets of conjugate operations which it contains are congruent to each other (mod. 16).

The chief result of the second section is that a group of prime degree which is not doubly transitive must be metacyclical. It follows that there are no simple groups of odd composite order and prime degree.

In the third section I have extended from degrees not exceeding 50 to degrees not exceeding 100 the result obtained by Dr. Miller,[*] viz., that corresponding to such degrees there are no simple groups of odd composite order. The method used is such that in only four cases, namely, for degrees 57, 81, 91, and 99, is any detailed discussion necessary; and I have no doubt that by it the lower limit for the degree of possible simple groups of odd composite order might, without much labour, be carried considerably beyond 100.

The results obtained in this paper, partial as they necessarily are, appear to me to indicate that an answer to the interesting question as to the existence or non-existence of simple groups of odd composite order may be arrived at by a further study of the theory of group-characteristics.

I.

1. A doubly transitive permutation group has obviously only two quadratic invariants, viz., the sum of the squares of its symbols and the sum of their products two together.

Let G be a simply transitive group in the symbols

$$x_1,\ x_2,\ \dots,\ x_n,$$

and let G_s be the sub-group of G which leaves x_s unchanged. G_s will interchange the remaining $n-1$ symbols in $m\,(\geq 2)$ transitive sets. For each suffix s these sets will be denoted by

$$\begin{array}{llll}
x_{s1,1}, & x_{s1,2}, & \dots, & x_{s1,k_1}, \\
x_{s2,1}, & x_{s2,2}, & \dots, & x_{s2,k_2}, \\
\dots & \dots & \dots & \dots \\
x_{sm,1}, & x_{sm,} & \dots, & x_{sm,k_m},
\end{array}$$

where one or more of the k's may be unity.

---

[*] *Proc. Lond. Math. Soc.*, Vol. xxxiii., pp. 6–10.

Suppose that S and S' are any two substitutions each of which changes x_1 into x_s, so that

$$S^{-1}G_1S = S'^{-1}G_1S' = G_s.$$

The set of symbols $x_{11,1}, x_{11,2}, \ldots, x_{11,k_1}$

which are interchanged transitively by G_1 must be changed by S into a set, equal in number, which are interchanged transitively by G_s. Hence it may be assumed that

$$S\,(x_{11,1}, x_{11,2}, \ldots, x_{11,k_1}) = (x_{s1,1}, x_{s1,2}, \ldots, x_{s1,k_1}).$$

Suppose, if possible, that

$$S'\,(x_{11,1}, x_{11,2}, \ldots, x_{11,k_1}) = (y_1, y_2, \ldots, y_{k_1}),$$

where the y's constitute some other set which are interchanged transitively by G_s. Then $S^{-1}S'$ changes the set

$$x_{s1,1}, x_{s1,2}, \ldots, x_{s1,k_1}$$

into the set $y_1, y_2, \ldots, y_{k_1}$.

But $S^{-1}S'$, leaving x_s unchanged, belongs to G_s; and the former set are interchanged transitively among themselves by G_s. Hence

$$S'\,(x_{1,11}, x_{11,2}, \ldots, x_{11,k_1}) = (x_{s1,1}, x_{s1,2}, \ldots, x_{s1,k_1}).$$

It follows that a correspondence may be established among the transitive sets in which the different sub-groups G_s interchange the symbols such that for all values of the suffixes s and t every operation of G which changes x_s into x_t also changes the set

$$x_{sp,1}, x_{sp,2}, \ldots, x_{sp,k_p}$$

into the set

$$x_{tp,1}, x_{tp,2}, \ldots, x_{tp,k_p}$$

$$(p = 1, 2, \ldots, m).$$

Consider now the quadratic function

$$f = \sum_{s=1}^{s=n} x_s\,(x_{s1,1}+x_{s1,2}+\ldots+x_{s1,k_1}).$$

It is clearly invariant for every operation of G; and, apart from a possible numerical factor, it is the smallest quadratic invariant of G which contains $x_sx_{s1,1}$. No one of the n brackets contains a repeated symbol, and every one of the n symbols must enter in the brackets the same number of times, viz., k_1. Hence, gathering together those products which have the same second symbol,

$$f = \sum_{s=1}^{s=n} (y_{s1}+y_{s2}+\dots+y_{sk_1})\, x_s,$$

and every operation of G_s must interchange among themselves the symbols in the bracket multiplying x_s. These symbols must, therefore, constitute one or more complete transitive sets for G_s; and, since, from the first form of f, there are substitutions in G which change any one product $x_s x_{s1,1}$ of f into any other, the y's must constitute a single transitive set of G_s. Suppose, first, that

$$(y_{s1}, y_{s2}, \dots, y_{sk_1}) = (x_{s1,1}, x_{s1,2}, \dots, x_{s1,k_1}).$$

Then every product of two symbols must occur twice in f, and therefore nk_1 must be even. If G is a group of odd order, this is impossible, and the two sets must be distinct. Hence, for a group of odd order the k's are equal in pairs and m is even. Further, m is clearly congruent to 0 or 2 (mod. 4), according as n is congruent to 1 or 3 (mod. 4); and the number of independent quadratic invariants is $1+\frac{m}{2}$. For a group of even order

$$(y_{s1}, y_{s2}, \dots, y_{sk_1}) = (x_{s1,1}, x_{s1,2}, \dots, x_{s1,k_1}),$$

if the group contains a substitution of order 2 which transposes x_s and $x_{s1,1}$. In this case no statement can be made as regards the parity of m, and the number of independent quadratic invariants is greater than $1+\frac{m}{2}$.

2. The result thus obtained for groups of odd order will now be applied to a particular case. Let g be a group of odd order n, represented as a regular permutation group in n symbols; and let g' be the simply isomorphic permutation group* in the n symbols, each of whose substitutions is permutable with every substitution of g. The group $\{g, g'\}$, whose order is n^2/n', where n' is the number of self-conjugate operations of g, is such that its sub-groups which leave one symbol unchanged interchange the remaining $n-1$ in $r-1$ sets (*loc. cit.*), where r is the number of conjugate sets in g. Since n is odd, r is odd, and the number of independent quadratic invariants of $\{g, g'\}$ is $\frac{1}{2}(r+1)$.

The group $\{g, g'\}$, being a permutation group, is reducible, and it is shown in my paper "On the Continuous Group defined by any given Group of Finite Order" (*Proc. Lond. Math. Soc.*, Vol. XXIX., pp. 558, 559) that the r sets of linear functions of the original variables, there denoted by

---

* *Theory of Groups*, p. 146.

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{im_i} \quad (i = 1, 2, \ldots, r),$$

are each transformed among themselves by the operations of $\{g, g'\}$. The total number of these linear functions is n; they are shown (*loc. cit.*) to be linearly independent. Since the original form of $\{g, g'\}$ is real, it follows that, if

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{im_i}$$

are transformed among themselves, so also are

$$\bar{\xi}_{i1}, \bar{\xi}_{i2}, \ldots, \bar{\xi}_{im_i},$$

where ξ and $\bar{\xi}$ are conjugate imaginaries.

Moreover, these $2m_i$ functions either must be linearly independent or each of one set must be linearly expressible in terms of the other set. In fact, if $m' (< m_i)$ linear functions of the second set were expressible in terms of the first set, these m' functions would be transformed among themselves by all the operations of $\{g, g'\}$, and therefore also by all operations of the continuous group $\{G, G'\}$; and this is shown (*loc. cit.*, p. 558) not to be the case.

Now, for every group of linear substitutions of finite order in m variables, at least one Hermitian form,

$$\Sigma a_{ij} x_i \bar{x}_j \quad (a_{ij} = \bar{a}_{ji}),$$

exists which is invariant for the group.* Let such a Hermitian form be constructed for each of the r sets of variables in which $\{g, g'\}$ has been expressed. If

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{im_i}$$

and $$\bar{\xi}_{i1}, \bar{\xi}_{i2}, \ldots, \bar{\xi}_{im_i}$$

are linearly independent, the Hermitian forms for these two sets are identical, and the two sets so give rise to a single real quadratic invariant for $\{g, g'\}$. If, on the other hand,

$$\bar{\xi}_{i1}, \bar{\xi}_{i2}, \ldots, \bar{\xi}_{im_i}$$

are expressible in terms of

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{im_i},$$

---

* This theorem was given independently by Prof. A. Loewy (*Comptes Rendus*, Vol. CXXIII., pp. 168–171), and by Prof. E. H. Moore (*Math. Ann.*, Vol. L., pp. 213–219).

then this single set gives rise to a real quadratic invariant for $\{g, g'\}$. Since, in any case,

$$\xi_{i1},\ \xi_{i2},\ \ldots,\ \xi_{im_i},\ \bar{\xi}_{i1},\ \ldots,\ \bar{\xi}_{im_i}$$

are linearly independent of the variables

$$\xi_{j1},\ \xi_{j2},\ \ldots,\ \xi_{jm_j}$$

belonging to any other distinct set, the quadratic invariant of $\{g, g'\}$ which arises from this latter set is essentially distinct from that which arises from

$$\xi_{i1},\ \xi_{i2},\ \ldots,\ \xi_{im_i}.$$

Now, when i is unity m_i is unity, and the corresponding ξ_{11} is real, viz., the sum of the original variables. This set by itself gives rise to one quadratic invariant, and therefore, unless the remaining $r-1$ sets occur in pairs, such as

$$\xi_{i1},\ \xi_{i2},\ \ldots,\ \xi_{im_i}$$

and

$$\bar{\xi}_{i1},\ \bar{\xi}_{i2},\ \ldots,\ \bar{\xi}_{im_i},$$

so that each pair gives rise to a single real quadratic invariant, the number of independent quadratic invariants would exceed $\frac{1}{2}(r+1)$. But $\frac{1}{2}(r+1)$ has been shown to be the number of such invariants. Hence for each value of i except unity

$$\xi_{i1},\ \xi_{i2},\ \ldots,\ \xi_{im_i},$$
$$\bar{\xi}_{i1},\ \bar{\xi}_{i2},\ \ldots,\ \bar{\xi}_{im_i}$$

are linearly independent; and therefore, with the same limitation,

$$\frac{1}{\chi_1^i}\sum_s h_s\chi_s^i\epsilon_s \quad \text{and} \quad \frac{1}{\chi_1^i}\sum h_s\bar{\chi}_s^i\epsilon_s,$$

the multipliers of these two sets of functions in H, are distinct.

In other words, a group of odd order has no self-inverse set of group-characteristics except the first; and therefore in each such set some at least of the characteristics must be imaginary.

This involves that when a group of odd order is represented as an irreducible group of linear substitutions some of the coefficients must be imaginary; or, that a group of odd order cannot be expressed in a form which is at once real and irreducible.

3. This result appears to me of such importance for the theory of groups of odd order that I give a second independent proof of it. Suppose, if possible, that every characteristic of a set, other than the

first, is real; and let the characteristic of an operation S of order m be

$$\chi_1 = a_0 + a_1(\omega + \omega^{-1}) + a_2(\omega^2 + \omega^{-2}) + \dots,$$

where ω is a primitive m-th root of unity, and $a_0, a_1, a_2, \dots$ are positive integers or zeroes. Then χ_1 is also the characteristic of S^{-1}, which belongs to the inverse set to that containing S. Moreover, if S^x (x prime relatively to m) does not belong to the same set as either S or S^{-1}, no more does S^{-x}; and, if the set containing S^x has χ_1 for its characteristic, so also has the set containing S^{-x}. Hence, of the conjugate sets containing powers of S whose indices are relatively prime to m, an even number 2μ must have χ_1 for characteristic. Suppose, now, that when ω is replaced by each primitive m-th root in turn χ_1 takes the s distinct values

$$\chi_1, \chi_2, \dots, \chi_s.$$

Then for each of these as characteristic there are 2μ conjugate sets containing powers of S whose indices are relatively prime to m; and the conjugate sets which contain such powers of S are thus exhausted. Moreover, the number of operations in each such set is the same. Hence $\Sigma h\chi$ for these sets is an even multiple of

$$\chi_1 + \chi_2 + \dots + \chi_s,$$

and this latter quantity is a rational positive or negative integer (or zero). Hence, for this system of conjugate sets $\Sigma h\chi$ is even. Now all the sets except the first may be arranged in such systems, and therefore $\Sigma h\chi$ for all conjugate sets except the first is even. Since the group is of odd order, the characteristic of the identical operation is necessarily odd; and the equation

$$\sum_{k=1}^{k=r} h_k \chi_k = 0^*$$

would involve that the sum of an even and an odd number is zero. This contradiction shows therefore that the supposition that all the characteristics of the set were real was incorrect; and hence that a group of odd order can have no self-inverse set of characteristics except the first.

From this result a relation between n, the order of the group, and r, the number of sets of conjugate operations, may be at once deduced.

---

* This relation is the particular case of the relation

$$\Sigma h_k \chi_k^i \chi_{k'}^j = 0,$$

which results from taking $j = 1$.

In fact, for two inverse sets

$$\chi_1^i = \chi_1^{i'} = 2k+1, \text{ an odd number.}$$

Hence $$(\chi_1^i)^2 + (\chi_1^{i'})^2 = 2\,(2k+1)^2 \equiv 2, \quad \text{mod. } 16;$$

and therefore, since $\chi_1^1 = 1$,

$$n = \sum_i (\chi_1^i)^2 \equiv r, \quad \text{mod. } 16.$$

Similarly, it may be shown that, if every factor of n is of the form $2km+1$, where m is an assigned odd integer, then

$$n \equiv r, \quad \text{mod. } 16m.^*$$

4. The relation $$\sum_i \chi_k^i \chi_l^i = 0, \quad l \neq k',$$

becomes for a group of odd order, by taking k for l,

$$\sum_i (\chi_k^i)^2 = 0,$$

and, combining this with $\sum_i \chi_k^i \chi_{k'}^i = \dfrac{n}{h_k}$,

$$-\sum_i (\chi_k^i - \chi_{k'}^i)^2 = \sum_i (\chi_k^i + \chi_{k'}^i)^2 = \frac{2n}{h_k}.$$

As an application of these formulæ, I consider a group whose order is divisible by 3, and I suppose the order of the operations of the k-th set to be 3. Then

$$\chi_k^i = a_0^i + a_1^i\,\omega + a_2^i\,\omega^2,$$

where ω is a primitive cube root of unity and a_0^i, a_1^i, a_2^i are positive integers or zeroes,

$$\chi_k^i - \chi_{k'} = (a_1^i - a_2^i)\,\sqrt{-3},$$

and therefore $$3\sum_i (a_1^i - a_2^i)^2 = \frac{2n}{h_k} = 2m_k,$$

---

* For the smaller values of r the determination of all groups of odd order with a given number of conjugate sets presents no difficulty. Thus for values of r less than 16 the only groups of odd order which have no self-conjugate operations are the following:—For $r = 5$, $n = 7 \cdot 3$; $r = 7$, $n = 11 \cdot 5$, $13 \cdot 3$; $r = 9$, $n = 19 \cdot 3$; $r = 11$, $n = 5^2 \cdot 3$, $31 \cdot 5$, $29 \cdot 7$, $19 \cdot 9$; $r = 13$, $n = 31 \cdot 3$, $41 \cdot 5$, $43 \cdot 7$, $37 \cdot 9$, $23 \cdot 11$, $3^4 \cdot 13$; $r = 15$, $n = 37 \cdot 3$, $3^3 \cdot 13$. These groups are all metacyclical with the exception of those of orders $5^2 \cdot 3$, $3^3 \cdot 13$, and $3^4 \cdot 13$. This list is in marked contrast to the corresponding one for groups of even order. Again, omitting groups with self-conjugate operations, the latter is:—for $r = 3$, $n = 3 \cdot 2$: $r = 4$, $n = 5 \cdot 2$, $2^2 \cdot 3$; $r = 5$, $n = 7 \cdot 2$, $5 \cdot 2^2$, $2^3 \cdot 3$, $2^2 \cdot 3 \cdot 5$; $r = 6$, $n = 3^2 \cdot 2$, two types, $3^2 \cdot 2^2$, $2^3 \cdot 3 \cdot 7$. In this list two simple groups appear, though the number of conjugate sets does not exceed 6.

where m_k is the order of the greatest sub-group which contains one of the operations of the k-th set self-conjugately. Hence, unless m_k is a multiple of 27, there must be at least one pair of inverse sets of characteristics for which $a^i_1 - a^i_2$ is not a multiple of 3. The product of the multipliers for such a set would be $\omega^{a^i_1 - a^i_2}$, that is ω or ω^2; and the group therefore would have a self-conjugate sub-group of index 3, formed by those operations for which the product of the multipliers is unity. In particular a group of order $3m$ or 3^2m, where m is odd and prime relatively to 3, has a self-conjugate sub-group of order m. Suppose now that 5 is a factor of the order, and that the k-th set is of order 5. Then

$$\chi^i_k = a^i_0 + a^i_1\epsilon + a^i_2\epsilon^2 + a^i_3\epsilon^3 + a^i_4\epsilon^4,$$

where ϵ is a primitive fifth root of unity and

$$\chi_k - \chi^i_{k'} = (a^i_1 - a^i_4)(\epsilon - \epsilon^4) + (a_{\cdot} - a^i_3)(\epsilon^2 - \epsilon^3).$$

If this is not zero, there must be a second set for which

$$\chi^j_k - \chi^j_{k'} = (a^i_1 - a^i_4)(\epsilon^2 - \epsilon^3) + (a^i_2 - a^i_3)(\epsilon^4 - \epsilon),$$

and $$(\chi^i_k - \chi^i_{k'})^2 + (\chi^j_k - \chi^j_{k'})^2 = -5\left\{(a^i_1 - a^i_4)^2 + (a^i_2 - a^i_3)^2\right\}.$$

Hence $$5\Sigma\left\{(a^i_1 - a^i_4)^2 + (a^i_2 - a^i_3)^2\right\} = 2m_k,$$

where the summation is extended to all pairs of sets such as the i-th and j-th. If m_k is not divisible by 5^2, there must be at least one set for which

$$(a^i_1 - a^i_4)^2 + (a^i_2 - a^i_3)^2 \not\equiv 0, \quad \text{mod. } 5;$$

and therefore $$a^i_1 - a^i_2 + 2(a^i_2 - a^i_2) \not\equiv 0, \quad \text{mod. } 5.$$

For such a set the product of the multipliers of an operation of the k-th set is a primitive fifth root of unity. Moreover, if 5 is an unrepeated factor of the order, m_k cannot be divisible by 25. Hence, a group of order $5m$, where m is odd and prime relatively to 5, has a self-conjugate sub-group of order m.

II.

5. In his memoir "Über die Darstellung der endlichen Gruppen durch lineare Substitutionen" (*Berliner Sitzungsberichte*, 1897, pp. 994–1015) Herr Frobenius has proved the theorem that, if two groups of linear substitutions in the same number of variables are simply isomorphic, and if the sums of the multipliers of corresponding operations in the two groups are the same, then the one group is

the result of transforming the other by some substitution of non-vanishing determinant. This theorem is clearly of fundamental importance in dealing with groups of finite order. In any representation of a group as a group of linear substitutions the sum of the multipliers for every operation of the k-th conjugate set is of the form $\Sigma a_i \chi_k^i$, where a_i is a positive integer (or zero) which is the same for all the sets, and $\Sigma a_i \chi_1^i$ is the number of variables (*Proc. Lond. Math. Soc.*, Vol. XXIX., pp. 564, 565). Hence, by taking a_i sets of χ_1^i variables for each suffix i, and forming in each set the irreducible group which has the characteristics $\chi_1^i, \chi_2^i, \ldots, \chi_r^i$, a group of linear substitutions is set up simply isomorphic with the given group, and having the same total number of variables and the same sum of the multipliers for each operation that the given group has. The theorem therefore shows the possibility of transforming any group of linear substitutions of finite order in such a way as to represent it as the result of an isomorphism established among a number of irreducible groups in independent sets of variables. These irreducible groups will here be spoken of as the irreducible *components* of the given group of linear substitutions. Apart from transformations of the irreducible components themselves, this reduction will be a unique process if no one of the irreducible components is repeated, but not otherwise.

A permutation group is never irreducible. In fact, the sum of the variables is unaltered by every operation of the group. If

$$x_1, x_2, \ldots, x_n$$

are the variables of a permutation group g, and if

$$\xi_1, \xi_2, \ldots, \xi_m$$

are a set of linear functions of the x's which are transformed among themselves by an irreducible component of g of which

$$\chi_1, \chi_2, \ldots, \chi_r$$

are the characteristics, then

$$\bar{\xi}_1, \bar{\xi}_2, \ldots, \bar{\xi}_m$$

must be linearly transformed among themselves by an irreducible component whose characteristics are

$$\bar{\chi}_1, \bar{\chi}_2, \ldots, \bar{\chi}_r.$$

For a group of even order this may be the same component as the previous one, but for a group of odd order it is necessarily distinct. For a transitive group of odd order the number of irreducible components is therefore odd and congruent (mod. 4) to the degree of the group. Moreover, since the coefficients of a permutation group are all rational, it follows that, if it has an irreducible component for which the characteristics are

$$\chi_1, \chi_2, \dots, \chi_r,$$

it must have irreducible components whose characteristics,

$$\chi_1', \chi_2', \dots, \chi_r',$$

are derived from the previous set by replacing any irrationality that occurs in them by one of its conjugate values.

6. Let g be a transitive permutation group in the n symbols

$$x_1, x_2, \dots, x_n.$$

When the reduction of g is completely effected, let

$$\begin{array}{l} \xi_{11} \qquad (= x_1 + x_2 + \dots + x_n); \\ \xi_{21}, \xi_{22}, \dots, \xi_{2m_2}; \\ \dots \quad \dots \quad \dots \quad \dots \\ \xi_{k1}, \xi_{k2}, \dots, \xi_{km_k} \end{array}$$

be the sets of symbols which are transformed, each among themselves, by irreducible components of g; so that the ξ's form a set of n independent linear functions of the x's. Every operation of the continuous Abelian group H,

$$\xi_{si}' = a_s \xi_{si}$$
$$(i = 1, 2, \dots, m_s),$$
$$(s = 1, 2, \dots, k),$$

is permutable with every operation of g. This continuous group H is not, however, necessarily the most extensive group every one of whose operations is permutable with every operation of g. In fact, if two (or more) sets of the ξ's, such as

$$\xi_{i1}, \xi_{i2}, \dots, \xi_{im_i}$$

and $$\xi_{j1}, \xi_{j2}, \dots, \xi_{jm_j},$$

contain the same number of symbols (so that $m_i = m_j$), and if these two sets undergo identical transformations corresponding to the same substitution of g, then

$$\xi_{st}' = \xi_{st} \quad (s \neq i, j),$$

$$\left. \begin{array}{l} \xi_{it}' = \alpha \xi_{it} + \beta \xi_{jt} \\ \xi_{jt}' = \gamma \xi_{it} + \delta \xi_{jt} \end{array} \right\} \quad (t = 1, 2, \dots m_i)$$

is a linear substitution not contained in H, and permutable with every operation of g. No such linear substitution, however, is permutable with every operation of H; and therefore, if such substitutions exist, the most general continuous group G each of whose operations is permutable with every operation of g is not Abelian.

Conversely, if the most general continuous group G whose operations are permutable with every operation of g is Abelian, it must be the group H; and each set of functions which occur in connexion with the same multiplier in H are transformed among themselves by an irreducible component of g.

The form of G, in terms of the x's, may be obtained as follows. Let

$$x'_r = x_{r'} \quad (r = 1, 2, \dots, n)$$

be any operation of g. The linear substitution

$$x'_r = \sum_{s=1}^{s=n} a_{rs} x_s \quad (r = 1, 2, \dots, n)$$

will be permutable with this operation if

$$\left.\begin{array}{ll} & x'_r = \sum_{s=1}^{s=n} a_{rs} x_{s'} \\ \text{and} & x'_r = \sum_{s=1}^{s=n} a_{r's} x_s \end{array}\right\} \quad (r = 1, 2, \dots, n)$$

are the same substitution; that is, if

$$a_{rs} = a_{r's'} \quad (r, s = 1, 2, \dots, n),$$

$x_{r'}$ and $x_{s'}$ being the symbols in which x_r and x_s are changed by the operation of g considered. Hence the necessary and sufficient condition that

$$x'_r = \sum_{s=1}^{s=n} a_{rs} x_s \quad (r = 1, 2, \dots, n)$$

should be permutable with every operation of g is that the coefficients a_{rs} should be equal in sets; any two a_{rs} and a_{pq} being equal if g contains a substitution which changes x_r and x_s into x_p and x_q respectively.

Since g is transitive, $a_{11} = a_{22} = \dots = a_{nn}$,

and no one of these symbols is equal to a_{rs}, if r and s are different. If g is doubly transitive,

$$a_{rs} = a_{pq},$$

where r, s and p, q are any two pairs of distinct symbols; and the general operation of G takes the form

$$x'_r = (a-b)\, x_r + b \sum_1^n x_s \quad (r = 1, 2, \dots, n).$$

If g is not doubly transitive, the general operation of G, with the notation of p. 163, will be

$$x'_s = a_0 x_s + \sum_{t=1}^{t=m} a_t (x_{st,1} + x_{st,2} + \ldots + x_{st,k_t})$$

$$(s = 1, 2, \ldots, n).$$

The order of G is, therefore, $m+1$, where m is the number of transitive sets in which a sub-group of g that leaves one symbol unchanged interchanges the remaining $n-1$, and the number of irreducible components of g is equal to or is less than $1+m$, according as G is or is not Abelian. It may be noticed that the necessary and sufficient condition that G should contain a permutation is that at least one of the numbers $k_1, k_2, \ldots, k_m$ should be unity; *i.e.*, that a sub-group of g which leaves one symbol unchanged leaves more than one. If G is not Abelian, g must have at least three irreducible components; and, if G is Abelian, the number of irreducible components of g is equal to the order of G. Hence, g must have more than two irreducible components, unless it is doubly transitive; and, if g is doubly transitive, it has just two irreducible components. One of these is the component of order unity corresponding to the sum of the variables, and the other may be represented as a group of linear substitutions in the $n-1$ differences

$$x_1 - x_n,\ x_2 - x_n,\ \ldots,\ x_{n-1} - x_n.$$

It is not difficult to show that, if g is primitive, then G must be Abelian.

7. Let g be a simply transitive substitution group of prime degree p containing the operation P or

$$(x_0 x_1 \ldots x_{p-1}),$$

and let g be resolved into its irreducible components in such a way that in each of them P appears in canonical form. In the first component corresponding to the sum of the variables the multiplier of P is unity. Hence, in any other component the multipliers of P must be distinct primitive p-th roots of unity. Let

$$\xi'_{it} = \omega_{it} \xi_{it} \quad (t = 1, 2, \ldots, m_i)$$

be the operation corresponding to P in the $(i+1)$-th irreducible component $(i = 1, 2, \ldots, s)$. There is only one linear function of the variables which P replaces by ω_{it} times itself, viz.,

$$x_0 + \omega_{it}^{-1} x_1 + \omega_{it}^{-2} x_2 + \ldots + \omega_{it}^{-p+1} x_{p-1}.$$

This therefore must be ξ_{it}, and the $p-1$ ξ's of this form, corresponding to the $p-1$ primitive p-th roots of unity, are transformed linearly among themselves in s distinct sets by the irreducible components, other than the first. The coefficients in these linear substitutions are rational functions of any assigned p-th root of unity ω. If ω is replaced by any other primitive root ω', the sets of linear substitutions giving g in its reduced form is unaltered as a whole, but individual components may be interchanged.

Consider now the characteristic of P (*i.e.*, the sum of its multipliers) in one of the components, viz.,

$$\omega_{i1}+\omega_{i2}+\ldots+\omega_{im_i}.$$

When ω' is written for ω this is either unchanged or it becomes another characteristic of P. Hence, since P has no repeated multipliers, this expression must be a "period" in the cyclotomic sense; and m_i must have the same value r for each of the irreducible components, where

$$rs=p-1.$$

Also, if q is a primitive root of the congruence

$$q^r\equiv 1 \pmod p,$$

and if
$$\xi_i=x_0+\omega^i x_1+\omega^{2i}x_2+\ldots+\omega^{(p-1)i}x_{p-1},$$

the form which any operation of g takes when expressed in terms of the ξ's is

$$\xi'=c^t_{11}\xi_t+c_{12}\xi_{tq}+\ldots+c^t_{1r}\xi_{tq^{r-1}},$$
$$\ldots\quad\ldots\quad\ldots\quad\ldots\quad\ldots$$
$$\xi_{tq^{r-1}}=c^t_{r1}\xi_t+c^t_{r2}\xi_{tq}+\ldots+c^t_{rr}\xi_{tq^{r-1}},$$
$$(t=1,2,\ldots,s).^*$$

Since the ξ's are linear functions of the x's with powers of ω as coefficients, the coefficients c^t_{ij} in this substitution are rational functions of ω. Moreover, since by writing ω^t for ω,

$$\xi_1,\ \xi_q,\ \ldots,\ \xi_{q^{r-1}}$$

become
$$\xi_t,\ \xi_{tq},\ \ldots,\ \xi_{tq^{r-1}},$$

c^t_{ij} must be the same function of ω^t as c^1_{ij} is of ω.

---

* The t in c^t_{ij} is not an index, but merely an affix.

Consider now any operation of g whose order, q, is different from and necessarily prime to p. Its characteristic in the t-th component,

$$c^t_{11}+c^t_{22}+\dots+c^t_{rr},$$

is the sum of r q-th roots of unity. But this sum is also a rational function of ω. Hence it must be a rational number, and therefore independent of t. Moreover, this sum, being a characteristic, is an algebraical integer; and therefore, being a rational number, it is a rational integer. Represent it by χ. Then $1+s\chi$ is the sum of the multipliers (*i.e.*, the number of unchanged symbols) of the operation in g. If this were zero, χ could not be integral; if it is unity, χ is zero; and, if it is greater than unity, χ is a positive integer. Hence, the only operations of g which displace all the symbols are the operations of order p, and every other operation of g leaves $1+s\chi$ symbols unchanged, where χ is zero or a positive integer. In each of the s irreducible components, other than the first, that arise from the reduction of g the characteristic of any conjugate set whose order is prime to p is then the same positive integer; and the characteristics of a conjugate set whose order is p are the s values of

$$\omega+\omega^q+\dots+\omega^{q^{r-1}},$$

when for ω each p-th root is put in turn. Let x be the number of conjugate sets whose characteristic in any one irreducible component is

$$\omega+\omega^q+\dots+\omega^{q^{r-1}},$$

and ν the number of operations in each set. Also, let ν_t be the number of operations of g which leave just t symbols unchanged, so that ν_t is zero, unless t is of the form $1+s\chi$. Then the equation

$$\sum_k h_k\chi^i_k = 0,$$

connecting a set of characteristics becomes

$$0 = -x\nu+\nu_{1+s}+2\nu_{1+2s}+\dots+r\nu_{1+rs}.$$

Also the equation $\qquad \sum_k h_k\chi^i_k\chi^j_{k'} = 0 \quad (i \neq j),$

becomes

$$0 = x\nu\Sigma\,(\omega+\omega^q+\dots+\omega^{q^{r-1}})(\omega^{-t}+\omega^{-tq}+\dots+\omega^{-tq^{r-1}})$$
$$+\nu_{1+s}+2^2\nu_{1+2s}+\dots+r^2\nu_{1+rs},$$

where the sum is extended to the s different values of the product.

To the condition $i \neq j$ corresponds the condition that the "periods"

$$\omega + \omega^q + \ldots + \omega^{q^{r-1}}$$

and

$$\omega^i + \omega^{iq} + \ldots + \omega^{iq^{r-1}}$$

are distinct; and with this limitation the sum is easily shown to be equal to $-r$. Hence, eliminating $x\nu$ between the two equations,

$$r(\nu_{1+s} + 2\nu_{1+2s} + 3\nu_{1+3s} + \ldots + r\nu_{1+rs}) = \nu_{1+s} + 2^2\nu_{1+2s} + 3^2\nu_{1+3s} + \ldots + r^2\nu_{1+rs}.$$

This relation can only be satisfied by

$$\nu_{1+s} = \nu_{1+2s} = \ldots = \nu_{1+(r-1)s} = 0;$$

or, in words, the substitution group g has no operations, except identity, which leave more than one symbol unchanged. The order of such a group must be pr, where r is a factor of $p-1$, and it contains a single sub-group of order p.

A transitive group of prime degree must therefore be either doubly transitive or metacyclical.

In particular, a group of odd order and prime degree is metacyclical.

8. Let g be a group of odd order and degree p^2, where p is a prime, and suppose that g contains an operation P of order p^2. If ω is a p^2-th root of unity, the characteristic χ of P in an irreducible component of g, other than the first, is a sum of powers of ω, none being repeated. Suppose, if possible, that χ contains both ω and ω^p. Since ω^p is unaltered by writing ω^{1+p} for ω, χ must also contain ω^{1+p}, ω^{1+2p}, ..., $\omega^{1+(p-1)p}$. If this does not exhaust all the p^2-th roots entering in χ, and if χ contains ω^t, then it must also contain $\omega^{t(1+p)}$, $\omega^{t(1+2p)}$, ..., $\omega^{t[1+(p-1)p]}$, and ω^{tp}. The total number of roots of unity entering in χ would, therefore, be a multiple of $p+1$, which is impossible, since this number must be odd. Hence, that characteristic which contains ω cannot contain ω^p. There must, therefore, be a characteristic in which all the multipliers are p-th roots of unity. The group therefore must be composite and isomorphic with a group in which P is represented by an operation of order p; in other words, g is imprimitive, and therefore, by the foregoing result, soluble.

A similar result may be proved for a group of odd order and degree pq, where p and q are primes, which contains a regular substitution S of order pq. Let ω and ω' be primitive p-th and q-th roots of unity. Then, if χ is the characteristic of S in one of the irreducible components of the group, ω and ω' cannot both occur in χ. For, if they did, since ω is unaltered on replacing ω' by any other primitive

q-th root, ω', ω'^2, ..., ω'^{q-1} would all occur; and this is impossible, since the roots composing $\bar{\chi}$, the inverse characteristic, must all be distinct from those composing χ. If $\omega\omega'$ and ω occur in χ, then in the characteristics derived from χ on replacing ω' by any other primitive q-th root every primitive pq-th root and every primitive p-th root occur. Hence there must then be other characteristics which consist solely of q-th roots. So also, if $\omega\omega'$ and ω' occur in χ, there must be characteristics which consist solely of p-th roots. The group is therefore composite, and isomorphic with a group in which S is represented by an operation of prime order; in other words, g is imprimitive, and therefore soluble. Hence:—

A transitive group of odd order, and degree p^2 or pq where p and q are primes, which contains a regular substitution of order equal to the degree is imprimitive and soluble.

It appears highly probable that this result may be extended to any group of odd order which contains a regular substitution of order equal to the degree of the group; but I have not yet succeeded in proving this.

III.

9. In conclusion, I propose to determine all the primitive groups of odd order and degree not exceeding 100. Dr. Miller sent me a paper four months ago for communication to the Society, in which an investigation, almost equivalent to this, was carried out for degrees not exceeding 50. The method I follow is, to a considerable extent, distinct from Dr. Miller's, and I have therefore allowed myself to repeat the investigation already given by him for degrees less than 50. This occupies but a small space, and serves to make the nature of the process clear.

In consequence of the theorem proved above for groups of prime degree, it is only necessary to consider those groups whose degrees are not primes. The method of the enumeration is as follows:—It is assumed that corresponding to a given odd number n as degree a primitive group g exists. Then a sub-group, g_0, which leaves one symbol unchanged must (p. 165) interchange the remaining $n-1$ symbols in $2m$ transitive sets, the numbers in which are equal in pairs. These numbers are represented by

$$k_1,\ k_2,\ \dots,\ k_{2m}.$$

Moreover, $$2m \equiv n-1 \pmod{4}.$$

Corresponding to each available value of m there will be a number of sets of values of the k's which may be written down. No k can be unity, for the group would then be imprimitive. Now Jordan has shown (" Traité des Substitutions," p. 284) that every prime which divides the order of one of the transitive constituents of g_0 must divide the order of each transitive constituent. On this ground, a large number of the sets of values of the k's may be put aside at once as impossible, including all those cases in which two k's are equal to different primes. Moreover, the earlier determinations increase the number of cases that may be so put aside in the later ones. For instance, it is found at once that there is no transitive group of odd order, and degree 9 or 15, whose order is divisible by 7; so that 7 and 9, or 7 and 15, are incompatible values for two k's. If each k is the same prime, every transitive constituent of g_0 is a metacyclical group. In this case, g_0 is metacyclical and simply isomorphic with each of its transitive constituents. This is an immediate consequence of a theorem due to Dr. Miller (*Proc. Lond. Math. Soc.*, Vol. XXVIII., p. 534, Theorem I.). When all impossible sets of values of the k's have been put aside, the orders of possible groups g corresponding to the remainder are of known form. These are separately discussed, with a view to showing that they are soluble. If n is not the power of a prime, a primitive group of degree n is not soluble. Hence, if it is shown that a group corresponding to a given possible order is soluble, the group is non-existent when n is not the power of a prime.

The number of cases which have to be thus dealt with is not considerable, but some of the more troublesome ones may be avoided by the following considerations:—If $m = 1$, the number of irreducible components of the group is 3 (p. 174). Suppose, now, that the group contains an operation of prime order p ($\equiv 1$, mod. 4) which displaces all the symbols. If χ is its characteristic in one of the irreducible components (other than that corresponding to the sum of the symbols, for which the characteristic is unity), then χ', the conjugate of χ, is its characteristic in the other irreducible component; and $\chi+\chi'+1$, the sum of the multipliers of the operation, is zero, since the operation displaces all the symbols. Hence, χ cannot be real. But, if χ is imaginary, it must be at least a four-valued function of the p-th roots of unity; and the four corresponding irreducible representations of the group would necessarily appear among the irreducible components of g. This is impossible; and, therefore, for a group which contains a substitution, regular in all the symbols and of prime order p ($\equiv 1$, mod. 4), m cannot be unity.

I now proceed to the actual enumeration. This is given in some detail for the smaller values of n; but for the larger ones, except when special discussion is necessary, the results are merely stated.

10. $n = 9$. There is no available value of m; so that the group must be imprimitive. Its order is 3^2, 3^3, or 3^4.

$n = 15$. The only available value of m is 1, and the k's are 7, 7. The order therefore would be 15.7 or 15.7.3, containing less than 6 prime factors. The group, therefore, would be soluble,* which is impossible. Hence the group must be imprimitive. The possible orders are 3.5, 3.5^2, 3.5^3, $3^4.5$, or $3^5.5$.

$n = 21$. Then $m = 2$, and the k's are 5, 5, 5, 5 or 3, 3, 7, 7. The second case is impossible. In the first the order would be 21.5, and, for the same reason as in the previous case, such a group cannot exist. The group is therefore imprimitive.

$n = 25$. If $m = 2$, the k's would be 5, 5, 7, 7 or 3, 3, 9, 9, each of which is impossible. If $m = 4$, the k's are all 3, and the order is 25.3. There is such a primitive group. All other groups of this degree must be imprimitive, their orders being powers of 5.

$n = 27$. If $m = 1$, the k's are 13, 13. The order, then, is 27.13 or 27.13.3. Primitive groups of these orders exist, containing self-conjugate sub-groups of order 27. If $m = 3$, the k's are 3, 3, 3, 3, 7, 7 or 3, 3, 5, 5, 5, 5, both of which are impossible. All other groups of this order, then, are imprimitive and have powers of 3 for their order.

$n = 33$. If $m = 2$, the k's are 7, 7, 9, 9; 5, 5, 11, 11; or 3, 3, 13, 13, all of which are impossible. If $m = 4$, two k's at least are 3, which is, again, impossible. The group is therefore imprimitive.

$n = 35$. If $m = 1$, the k's are 17, 17, and the order 35.17, the product of 3 primes. There can be no such group. If m is 3 or 5, two k's must either be 3 or 5, leading, again, to impossibilities. The group is therefore imprimitive.

$n = 39$. If $m = 1$, the k's are 19, 19, and the order 39.19, 39.19.3, or 39.19.9; in each case the product of fewer than 6 primes. There can be no such groups. The values 3 or 5 of m lead to the same impossibilities as in the previous case. The group is, then, imprimitive.

$n = 45$. If $m = 2$, the k's are 11, 11, 11, 11; 9, 9, 13, 13; 7, 7, 15, 15;

---

* *Theory of Groups*, p. 367.

5, 5, 17, 17; or 3, 3, 19, 19. All of these are impossible except the first case. In that the order would be 45.11 or 45.11.5; and the group again therefore is non-existent. If m were 4 or 6, two k's would again be 3 or 5, leading to impossibilities. The group is imprimitive.

$n = 49$. If $m = 2$, the k's are 11, 11, 13, 13; 9, 9, 15, 15; 7, 7, 17, 17; 5, 5, 19, 19; or 3, 3, 21, 21; all of which are impossible. If m is 4 or 6, two k's at least must be 3 or 5, leading to impossibilities. If $m = 8$. the k's are all 3. No primitive group of order 49.3 can exist; for a non-cyclical group of order 49 has 8 sub-groups of order 7, two at least of which must be transformed into themselves by an operation of order 3. The group is therefore necessarily imprimitive.

$n = 51$. If $m = 1$, the k's are 25, 25. The order of the sub-group that keeps one symbol fixed is of the form $3^{\alpha}.5^{\beta}$, and the group must contain an operation of order 17 which displaces all the symbols. It has been shown (p. 179) that this is inconsistent with the condition $m = 1$. If $m = 3$, the k's are 7, 7, 7, 7, 11, 11; 7, 7, 9, 9, 9, 9; which are impossible, or two k's are 3 or 5, leading to impossibilities. If $m = 5$, the k's are all 5, or two at least are 3, and, if $m = 7$, two k's at least are 3. All these cases are clearly impossible. The group is therefore imprimitive.

$n = 55$. If $m = 1$, the k's are 27, 27, and the order of the sub-group that keeps one symbol fixed is of the form $3^{\alpha}.13^{\beta}$. The group therefore has operations of order 5 which displace all the symbols, and this is inconsistent with the condition $m = 1$. If $m = 3$, the k's are 9, 9, 9, 9, 9, 9; 7, 7, 7, 7, 13, 13; 7, 7, 9, 9, 11, 11; or two k's at least are 3 or 5. The only possibility is the first, in which case the order of the group is $3^{\alpha}.5.11$. Such a group contains a self-conjugate sub-group of order $3^{\alpha-1}$ or $3^{\alpha-2}$, and could not be expressed as of degree 55. If m is 5, 7, or 9, two k's at least are 3 or 5, leading to impossibilities. Hence the group is imprimitive.

$n = 57$. If $m = 2$, the k's are 13, 13, 15, 15; 11, 11, 17, 17; 9, 9, 19, 19; 7, 7, 21, 21; 5, 5, 23, 23; or 3, 3, 25, 25; of which 7, 7, 21, 21 is the only set giving a possible group. The order of the sub-group that keeps one symbol fixed is of the form $3^{\alpha}.7^{\beta}$, and the order of the group itself is $3^{\alpha+1}.7^{\beta}.19$. If β is unity, there must be 7.19 sub-groups of order $3^{\alpha+1}$. Any two of these must have a common sub-group of order 3^{α}, and this must be self-conjugate in a sub-group of order $3^{\alpha+1}.7$, $3^{\alpha+1}.19$, or $3^{\alpha+1}.7.19$. In either case the group would be soluble, and it is therefore non-existent. Next suppose $\beta > 1$. The sub-groups of order 7^β are Abelian, and of degree 56. The greatest sub-group, g, common to two of them must keep $1+7x$ symbols fixed. Each of the corresponding sub-groups that keep one symbol fixed, and no others, has at least one sub-group of order 7^β which contains g. Hence, the order of the sub-group which contains g self-conjugately is divisible by $1+7x$. Now the only number of this form which is a factor of the order and not greater than the degree of the group is the degree itself; so that g is self-conjugate. Hence, again, in this case the group is non-existent. If m is 4, each k is 7, or two k's at least are 3 or 5; if $m > 4$, two k's at least are 3 or 5; and in all these cases the group is clearly non-existent. Hence the group must be imprimitive.

$n = 63$. If $m = 1$, the k's are 31, 31, and the order of the group 63.31, 63.31.3, 63.31.5, or 63.31.15. The last is the only one in which the order has 6 prime factors. Now, a group of order $3^3.5.7.31$ must contain a sub-group of order $3^3.5$, and in this a sub-group of order 5 must be self-conjugate. The group then would contain 1 or 31 sub-groups of order 5 and would be soluble. If $m = 3$, all sets of values of the k's lead to impossibilities. If m is 5, or greater, two k's at least must be 5 or 3. Hence the group must be imprimitive.

$n = 65$. Whatever m is, all sets of k's are found to lead to impossibilities. The group is imprimitive.

$n = 69$. If $m = 2$, the only possible set of values of the k's is 17, 17, 17, 17. The order of the corresponding group would be 3.17.23, containing only 3 prime factors, and therefore necessarily soluble. All other values of m lead to impossible sets of values of the k's. The group is, then, imprimitive.

$n = 75$. If $m = 1$, the k's are 37, 37, and the order is 75.37, 75.7.3, or 75.37.9. The last alone contains 6 prime factors. A group of order $3^3.5^2.37$ must have a self-conjugate sub-group of order 5 or 5^2, and is therefore soluble. This case, then, cannot occur. All other values of m lead to impossible sets of values for the k's. The group is therefore imprimitive.

$n = 77$. If $m = 2$, the only possible values of the k's are 19, 19, 19, 19. The order is, then, 77.19, 77.19.3, or 77.19.9, in each case containing less than 6 prime factors. This case cannot occur, and all other values of m lead to impossibilities. The group, then, is imprimitive.

$n=81$. If $m=2$, the only possible values for the k's are 15, 15, 25, 25, and the order of the group is $3^{4+a}.5^{\beta}$ $(\beta \geqslant 2)$. The sub-groups of order 5^{β} are Abelian and of degree 80. The greatest sub-group, g, common to two of them must keep $1+5x$ symbols fixed. Each of the corresponding sub-groups which keep one symbol fixed must contain at least one sub-group of order 5^{β} in which g is self-conjugate; and the order of the greatest sub-group containing g self-conjugately is therefore divisible by $1+5x$. The only factor of the order of the group of this form which is not greater than 81 is 81. Hence g is self-conjugate, and the group non-existent. All values of m greater than 2 lead to impossibilities except $m=8$ and all the k's 5. There is, in fact, a primitive group of order 81.5, degree 81, and class 80. All other groups of this order are imprimitive.

$n=85$. The only sets of values of the k's which do not lead to impossibilities are 21, 21, 21, 21; 7, 7, 7, 7, 7, 7, 21, 21; and twelve 7's. In none of these cases is the order of the group divisible by 5^2. Hence (p. 170) the group contains a self-conjugate sub-group of index 5, which is intransitive. For a primitive group this is impossible. The group is therefore imprimitive.

$n=87$. If $m=1$, the k's are 43, 43, and the order is 87.43; 87.43.3; 87.43.7; or 87.43.21, in each case containing less than 6 prime factors. All other values of m lead to impossible sets of values for the k's. The group, then, is imprimitive.

$n=91$. If $m=1$, the k's are 45, 45. The order of a transitive constituent of degree 45 cannot be divisible by 13; and the group contains operations of order 13 which displace all the symbols. This has been shown (p. 179) to be inconsistent with the condition $m=1$. If $m=3$, the only possible values of the k's are 15, 15, 15, 15, 15, 15 and 9, 9, 9, 9, 27, 27. If m is 5, the only possible values for the k's are ten 9's. In the two latter cases the order of the group is $3^a.7.13$. Two sub-groups of order 3^a would have a common sub-group of order 3^{a-2} at least, and this would be one of 1, 7, 13, 21, or 39 conjugate groups. Groups of degree 21 and 39 have been shown to be imprimitive. Hence this case cannot occur. In the first case the order of the group is

$3^\alpha.5^\beta.7.13$. The groups of order 5^β are Abelian and of degree 90. If β is unity, the group may be shown, as in the previous case, to be non-existent. If β is greater than unity, the greatest sub-group, g, common to two groups of order 5^β must keep $1+5x$ symbols fixed, and the greatest sub-group which contains g self-conjugately must interchange the $1+5x$ symbols transitively. The only possible value of $1+5x$ is 81; and the group can contain no sub-group with a transitive constituent of degree 81. Hence this case cannot occur. No value of m greater than 5 gives a possibility. The group, then, is imprimitive.

$n = 93$. The only possible values for a set of k's are 23, 23, 23, 23. The order of the group is then 93.23 or $93.23.11$; in either case containing less than 6 primes. This case, then, is impossible, and the group is imprimitive.

$n=95$. If $m=1$, the k's are 47, 47, and the order contains less than 6 prime factors. No other value of m leads to possible values for a set of k's. The group, then, is imprimitive.

$n = 99$. If $m=1$, the k's are 49, 49, and the order of the group is $3^{2+\alpha}.7^\beta.11$, where β is equal to or greater than 2. If β were 2, the group would contain 7 or 49 sub-groups of order $3^{2+\alpha}.11$, and would be soluble. If $\beta > 2$, let g be a greatest sub-group of a group of order 7^β which leaves more than one symbol unchanged. Then g must leave $1+7x$ symbols unchanged; and the greatest sub-group, h, in which g is self-conjugate must interchange the $1+7x$ symbols among themselves. Moreover, the order of the constituent of h which affects these $1+7x$ symbols is divisible by 7, and no one of them is left unchanged by every operation of h. Hence, for some value of x' equal to or less than x, $1+7x'$ must be a factor of the order of the group. No such factor exists other than 99, and this case therefore is impossible. The only other possible values of a set of k's are two 7's and four 21's; eight 7's and two 21's; or fourteen 7's. In each case the order of the group is of the form $3^{2+\alpha}.7^\beta.11$; while the sub-groups of order 7^β are Abelian and of degree 98. If $\beta = 1$, the group would obviously be soluble; and, if $\beta > 1$, the method used for degrees 81 and 91 will show that the group cannot exist. The group is therefore imprimitive.

To sum up, the result of this enumeration shows that :—

Apart from metacyclical groups of prime degree, the only primitive groups of odd order whose degree is less than 100 are (i.) a group of degree 25 and order 25.3; (ii.) two groups of degree 27 and orders

27.13 and 27.13.3; and (iii.) a group of degree 81 and order 81.5. All groups of odd order whose degree is less than 100 are soluble.

[*Note, January* 15*th*, 1901.—Since the above enumeration was made, I have succeeded in showing that a group of odd order and degree $3p$, where p is an odd prime, is necessarily imprimitive. This result, of which I hope to give the proof in a subsequent paper, would materially lessen the number of cases that have to be considered.]

Conformal Space Transformations. *By* T. J. I'A. Bromwich.

Received November 6th, 1900. Read November 8th, 1900.

The basis of the following note is a very suggestive method given by the late Prof. Sophus Lie,[*] by which he found the expression for a rigid-body displacement, assuming only that the distance between consecutive points of the body remains constant in the displacement. A slight extension of the same method is applied here to find the conformal transformations of space; and we are led to Liouville's theorem that the most general conformal transformation is due to an inversion, a uniform magnification, and a rigid-body displacement (combined in various ways).[†]

Liouville's theorem was extended by Lie (in 1871) to space of any number of dimensions and to non-Euclidian spaces; Lie's methods differ entirely from Liouville's and from what follows.[‡] Lie has also given a determination of the infinitesimal conformal transformations of ordinary space, by connecting points in space with circles in a plane;* the final results are obtained from the properties of contact-transformations of the circles. Still another proof is given by Lie (*loc. cit.*, Kap. x., § 1, p. 419), starting from the fact that lines of zero length (for which $dx^2+dy^2+dz^2=0$) remain of zero length; it then follows that spheres must be transformed into spheres—in particular, point-spheres become point-spheres. Lie refers to a note of Liouville's of earlier date (1847) than that quoted above; but Liouville's remarks in 1850 seem to indicate that his former investigations were not quite satisfactory.

---

[*] *Geometrie der Berührungstransformationen*, Kap. vi., § 3, p. 206. A similar method was used by Beltrami for finding rigid-body displacements in a space of constant curvature; my authority is an abstract given in Darboux's *Bulletin* (t. xi., 1876), where it is stated that the original paper was presented to the Roman Academy (*dei Lincei*); but I have not been able to find it.

[†] Liouville, *Journal de Mathématiques*, t. xv., 1850, p. 103, where the theorem appears without proof; which will be found in his notes to Monge's *Applications de l'analyse à la géometrie* (Paris, 1850, p. 609). Another form of the proof is given by J. N. Haton de Goupillière (*Journal de l'Ecole Polytechnique*, t. xxv., 1867, p. 188). The theorem was rediscovered in 1872 by Clerk Maxwell (*Proc. Lond. Math. Soc.*, Vol. iv., p. 117; *Works*, Vol. ii., p. 297), whose method differs but little from Liouville's.

[‡] *Math. Annalen*, Bd. v.; and *Gött. Nach.*, May, 1871.

Since my work was completed, I have found that (for the case $n=3$) Mr. J. E. Campbell† has used the same analysis to solve a somewhat different problem; he investigates the groups which leave unaltered the differential equation

$$\left(\frac{\partial U}{\partial x}\right)^2+\left(\frac{\partial U}{\partial y}\right)^2+\left(\frac{\partial U}{\partial z}\right)^2=0,$$

and remarks that these must be the same as the groups for which

$$dx^2+dy^2+dz^2=0$$

is invariant. The latter are, of course, the transformations investigated here. Mr. Campbell's method of deducing the inversion-result differs from mine, and is, perhaps, less direct. Prof. Tait‡ has also obtained Liouville's theorem by the aid of quaternions.

First consider ordinary space ($n=3$). Let an infinitesimal conformal transformation be defined by

$$\delta x = X\delta t,\quad \delta y = Y\delta t,\quad \delta z = Z\delta t,$$

where X, Y, Z are functions of x, y, z to be determined. By definition of conformal transformations, the magnification is a function only of x, y, z, and not of the direction of the line-element; thus the ratio

$$\delta\, ds : ds$$

is independent of the ratios $dx : dy : dz$.

Now
$$\begin{aligned} ds.\delta ds &= dx.\delta dx+dy.\delta dy+dz.\delta dz \\ &= (dx.dX+dy.dY+dz.dZ)\,\delta t, \end{aligned}$$

and so the ratio
$$\frac{dx.dX+dy.dY+dz.dZ}{dx^2+dy^2+dz^2}$$

---

* *Loc. cit.*, Kap. x., § 2, p. 441.

† *Messenger of Mathematics*, Vol. xxviii., 1898, p. 97.

‡ *Trans. Roy. Soc. Edin.*, Vol. xxvii., 1874, p. 105; *Proc. Roy. Soc. Edin.*, Vol. ix., 1877, p. 527, and Vol. xix., 1892, p. 193; reprinted in *Papers*, Vol. i., pp. 176, 352, Vol. ii., p. 329.

is to be independent of $dx : dy : dz$. But

$$dX = \frac{\partial X}{\partial x}dx + \frac{\partial X}{\partial y}dy + \frac{\partial X}{\partial z}dz, \quad \&c.,$$

and so we find the conditions

$$\frac{\partial X}{\partial x} = \frac{\partial Y}{\partial y} = \frac{\partial Z}{\partial z} = f,$$

say, and

$$\frac{\partial Z}{\partial y} + \frac{\partial Y}{\partial z} = 0,$$

$$\frac{\partial X}{\partial z} + \frac{\partial Z}{\partial x} = 0,$$

$$\frac{\partial Y}{\partial x} + \frac{\partial X}{\partial y} = 0.$$

If we write $\theta = -\frac{\partial Z}{\partial y}, \quad \phi = -\frac{\partial X}{\partial z}, \quad \psi = -\frac{\partial Y}{\partial x},$

we shall have, by our conditions, the table of differential coefficients*

	x	y	z
X	f	$+\psi$	$-\phi$
Y	$-\psi$	f	$+\theta$
Z	$+\phi$	$-\theta$	f

Putting down the nine conditions

$$\frac{\partial^2 X}{\partial x \partial y} = \frac{\partial^2 X}{\partial y \partial x}, \quad \&c.,$$

we find, first, the three $\frac{\partial \theta}{\partial x} = \frac{\partial \phi}{\partial y} = \frac{\partial \psi}{\partial z} = 0,$ (A)

and, second, three pairs, one of which is

$$\frac{\partial f}{\partial z} = \frac{\partial \theta}{\partial y}, \quad \frac{\partial f}{\partial y} = -\frac{\partial \theta}{\partial z} \qquad \text{(B)}.$$

---

* Here the entry given by a row Y and a column x means the differential coefficient $\frac{\partial Y}{\partial x}$; and so on.

From (B) $$\frac{\partial^2 f}{\partial z \partial x} = \frac{\partial^2 \theta}{\partial x \partial y},$$

and so, using (A), we find $$\frac{\partial^2 f}{\partial z \partial x} = 0.$$

By symmetry, $$\frac{\partial^2 f}{\partial y \partial z} = 0, \quad \frac{\partial^2 f}{\partial x \partial y} = 0.$$

Again, from (B), $$\frac{\partial^2 f}{\partial y^2} = -\frac{\partial^2 \theta}{\partial y \partial z} = -\frac{\partial^2 f}{\partial z^2}.$$

Comparing this with the symmetrical forms, we see that

$$\frac{\partial^2 f}{\partial x^2} = 0 = \frac{\partial^2 f}{\partial y^2} = \frac{\partial^2 f}{\partial z^2}.$$

Hence f is a linear function only of x, y, z, and so let us put

$$f = 2\,(\alpha x + \beta y + \gamma z + \delta),$$

where α, β, γ, δ are constants.*

Then, from (A) and (B), we have

$$\frac{\partial \theta}{\partial x} = 0, \quad \frac{\partial \theta}{\partial y} = 2\gamma, \quad \frac{\partial \theta}{\partial z} = -2\beta;$$

so that $$\theta = 2\,(\gamma y - \beta z) + p,$$

where p is a constant. From symmetry,

$$\phi = 2\,(\alpha z - \gamma x) + q,$$

$$\psi = 2\,(\beta x - \alpha y) + r.$$

Then we have
$$\begin{aligned} dX &= f\,dx + \psi\,dy - \phi\,dz \\ &= 2\,(\alpha x + \beta y + \gamma z + \delta)\,dx \\ &\quad + \left[2\,(\beta x - \alpha y) + r\right] dy + \left[2\,(\gamma x - \alpha z) - q\right] dz, \end{aligned}$$

or $$X = 2x\,(\alpha x + \beta y + \gamma z + \delta) - \alpha\,(x^2 + y^2 + z^2) + ry - qz + a,$$

where a is a new constant. Similarly,

$$Y = 2y\,(\alpha x + \beta y + \gamma z + \delta) - \beta\,(x^2 + y^2 + z^2) + pz - rx + b,$$

$$Z = 2z\,(\alpha x + \beta y + \gamma z + \delta) - \gamma\,(x^2 + y^2 + z^2) + qx - py + c$$

---

* Lie's method for the rigid-body displacement differs from this only in the point that f may be assumed zero at first, so as to make $\delta ds = 0$.

Thus the group of infinitesimal conformal transformations is a ten-parameter group; which is a familiar result.*

It is not difficult to give a geometrical interpretation of the forms X, Y, Z. For the terms in p, q, r, a, b, c correspond to the six-parameter group of rigid-body displacements. To interpret the others, consider the two spheres

$$(x-x_0)^2+(y-y_0)^2+(z-z_0)^2=k^2,$$

$$\left[x-(x_0+dx_0)\right]^2+\left[y-(y_0+dy_0)\right]^2+\left[z-(z_0+dz_0)\right]^2=(k+dk)^2,$$

and invert with respect to these two (in this order). It is found that the point (x, y, z) receives a displacement δx, δy, δz, where

$$\delta x = dx_0+\frac{2}{k^2}(x-x_0)\left[(x-x_0)\,dx_0+(y-y_0)\,dy_0+(z-z_0)\,dz_0+k\,dk\right]$$
$$-\frac{1}{k^2}\,dx_0\left[(x-x_0)^2+(y-y_0)^2+(z-z_0)^2\right],$$

&c.

It will be readily seen that $(x_0 y_0 z_0)$ may now be taken to be the origin,† and then the displacements so obtained form a four-parameter group which is exactly equivalent to the terms unaccounted for in $X\delta t$, $Y\delta t$, $Z\delta t$.

Passing to the case of a finite displacement, it is clear that the most general conformal transformation of space is made up of two inversions‡ and rigid-body displacements; and it also follows that there are no infinitesimal conformal transformations of a type different from these known finite ones.

As remarked above, this result (for *finite* transformations) was found by Liouville and Maxwell; but their proofs indicate a conformal transformation by means of *one* inversion; which is not, of course, entirely correct from our present standpoint. For by one inversion an elementary volume is changed to a volume which is similar, but *perverted*;§ we can illustrate the point by a reference to the proposition in two dimensions, that the conformal representation[*]

---

* See Lie (*loc. cit.*, p. 443).

† For the retention of the other terms is only equivalent to a rigid-body displacement.

‡ If we choose to suppose the radii of the two spheres of inversion the same, it will be necessary to add a uniform magnification (which is the same as two inversions at concentric spheres).

§ Or has its left and right sides interchanged, as by a single reflection in a mirror.

$$z' = (\alpha z+\beta)/(\gamma z+\delta)$$

is equivalent to *two* inversions, or to one inversion and one reflection in a line.[†]

Consider next the problem in space of n dimensions with a line-element ds given by

$$ds^2 = dx_1^2+dx_2^2+\dots+dx_n^2.$$

Repeating our argument for the case $n=3$, we find the following equations $\frac{1}{2}(n-1)(n+2)$ in number:—

$$\frac{\partial X_1}{\partial x_1}=\frac{\partial X_2}{\partial x_2}=\dots=\frac{\partial X_n}{\partial x_n},$$

and
$$\frac{\partial X_r}{\partial x_s}+\frac{\partial X_s}{\partial x_r}=0 \quad \left(\begin{matrix} r,\ s=1,\ 2,\ \dots,\ n \\ r\neq s\end{matrix}\right).$$

These are the conditions that the infinitesimal transformation[‡]

$$\delta x_r = X_r\,\delta t \quad (r=1,\ 2,\ \dots,\ n)$$

may be conformal. To solve them let us write

$$a_{rs}=\frac{\partial X_r}{\partial x_s} \quad (r,\ s=1,\ 2,\ \dots,\ n),$$

and note that in general $a_{rs}\neq a_{sr}$, if $s\neq r$.

Our differential equations now tell us that a_{rr} is the same for all values of r, $=\theta$, say; and that

$$a_{rs}+a_{sr}=0 \quad (r\neq s).$$

From the definition of the a's we have

$$\frac{\partial a_{rs}}{\partial x_p}=\frac{\partial^2 X_r}{\partial x_s\,\partial x_p}=\frac{\partial a_{rp}}{\partial x_s},$$

---

[*] $z=x+iy$; α, β, γ, δ are complex.

[†] It may be asked if our method applies to two-dimensional problems. It is readily seen that, if $\delta x = X\delta t$, $\delta y = Y\delta t$ give a conformal transformation, then

$$\frac{\partial X}{\partial x}=\frac{\partial Y}{\partial y},\quad \frac{\partial X}{\partial y}+\frac{\partial Y}{\partial x}=0,$$

or $(X+iY)$ is a function of z $(=x+iy)$. Thus

$$\delta z=(X+iY)\,\delta t=f(z)\,\delta t,$$

and so the finite conformal transformation is

$$z'=\phi(z),$$

a fact which is well known.

[‡] As before, the X's are functions of the x's to be found by the differential equations.

and, in the same way,

$$\frac{\partial a_{sr}}{\partial x_p} = \frac{\partial a_{sp}}{\partial x_r}, \quad \frac{\partial a_{pr}}{\partial x_s} = \frac{\partial a_{ps}}{\partial x_r}.$$

Hence, if $p \neq r \neq s$, we have

$$\frac{\partial a_{sp}}{\partial x_r} = \frac{\partial a_{sr}}{\partial x_p} = -\frac{\partial a_{rs}}{\partial x_p} = -\frac{\partial a_{rp}}{\partial x_s} = +\frac{\partial a_{pr}}{\partial x_s} = +\frac{\partial a_{ps}}{\partial x_s} = -\frac{\partial a_{sp}}{\partial x_r},$$

where we use alternately the differential conditions and the conditions

$$a_{sr} + a_{rs} = 0.$$

Hence
$$\frac{\partial a_{sp}}{\partial x_r} = 0,$$

and it follows that a_{sp} contains only x_s and x_p. Again,

$$\frac{\partial a_{rs}}{\partial x_r} = \frac{\partial a_{rr}}{\partial x_s} = \frac{\partial \theta}{\partial x_s},$$

and, similarly,
$$\frac{\partial a_{sr}}{\partial x_s} = \frac{\partial \theta}{\partial x_r}.$$

Thus, as
$$a_{rs} + a_{sr} = 0,$$

we have
$$\frac{\partial^2 \theta}{\partial x_r^2} + \frac{\partial^2 \theta}{\partial x_s^2} = 0.$$

This will hold for every pair of suffixes $(r \neq s)$, and so

$$\frac{\partial^2 \theta}{\partial x_r^2} = 0 \quad (r = 1, 2, \ldots, n).$$

Further, a_{rs} does not contain x_p $(p \neq r,\ p \neq s)$; so

$$\frac{\partial^2 \theta}{\partial x_p \partial x_s} = \frac{\partial}{\partial x_p}\left(\frac{\partial a_{rs}}{\partial x_r}\right) = 0.$$

Hence θ is linear in the x's, and so we may write

$$\theta = 2\left(l_1 x_1 + l_2 x_2 + \ldots + l_n x_n + k\right).$$

It follows that
$$\frac{\partial a_{rs}}{\partial x_r} = \frac{\partial \theta}{\partial x_s} = 2l_s,$$

$$\frac{\partial a_{sr}}{\partial x_s} = \frac{\partial \theta}{\partial x_r} = 2l_r,$$

and so
$$a_{rs} = 2\left(l_s x_r - l_r x_s\right) + \alpha_{rs},$$

where the a's are constants subject to the conditions*

$$a_{rs}+a_{sr}=0.$$

It now follows that
$$\begin{aligned} dX_r &= \Sigma a_{rs}\,dx_s \qquad (s=1,2,\ldots,n) \\ &= (\theta\,dx_r + x_r\,d\theta) - 2l_r\Sigma x_s\,dx_s + \Sigma a_{rs}\,dx_s \end{aligned}$$
or
$$X_r = x_r\theta - l_r\Sigma x_s^2 + \Sigma a_{rs}x_s + m_r.$$

Thus we have a group of $\frac{1}{2}(n+1)(n+2)$ parameters, where the m's are new constants.

Just as before, we consider now two consecutive transformations of the type (J) given by

$$x_r' = c_r + k^2(x_r - c_r)/\left[\Sigma(x_s - c_s)^2\right] \quad (r,\ s=1,2,\ldots,n),$$

and it will be seen that the values of the X's can be produced by two transformations of the type J, together with a rigid-body displacement.† It is then obvious that the most general conformal finite transformation can be made up in the same way. Transformations of the type J may be called generalized inversions; they have the property that hyperspheres are changed by them into other hyperspheres.‡

Another extension may be made by introducing Riemann's idea of a space of constant curvature (4λ) for which the line-element is expressed by the equation§

$$ds^2 = \Sigma dx_r^2/\left[1+\lambda\Sigma x_r^2\right]^2.$$

If we apply to this line-element the methods already indicated, it will be found that the same differential equations appear again; and so our analytical results will hold good in this case also. The geometrical interpretation may be left to geometers.

[*Note, May 3rd*, 1901.—M. Gaston Darboux has recently published a simple proof of Liouville's theorem; see *Archiv der Math. u. Phys.*, Series 3, Bd. I., 1901, p. 34.]

---

* These conditions arise in order to give $a_{rs}+a_{sr}=0$.

† If the quantity k is the same in the two (J) displacements, we must also add a uniform magnification.

‡ It may be asked what is the reason for the distinction between the conformal types for $n=2$ and those for $n>2$. On going back to the analysis it will be seen that our proof that θ must be linear really depends on the fact that

$$\frac{\partial a_{rs}}{\partial x_p} = 0 \quad (p \neq r,\ p \neq s),$$

and clearly such conditions can only exist if there are at least three variables.

§ Riemann, *Ueber die Hypothesen welche der Geometrie zu Grunde liegen.*

On a Class of Plane Curves. By J. H. Grace. Communicated November 8th, 1900. Received November 13th, 1900.

1. The well known chain of theorems established by Clifford in his "Synthetic Proof of Miquel's Theorem" has been lately obtained by M. Paul Serret* in an outwardly very different manner. Whereas the fundamental consideration in Clifford's proof is a curve of class n touching the line at infinity $(n-1)$ times, the corresponding idea in M. Serret's papers is a curve of the n-th degree, having its asymptotes concurrent and parallel to the sides of a regular polygon. In the one the locus of the foci plays the same part as the locus of the point of concurrence of the asymptotes does in the other. In the following paper, by following out the ideas of M. Serret, I have established an infinite series of propositions regarding lines and circles in a plane. After I had obtained the results hereafter explained a paper was published by Morley† in which the same results are obtained by purely analytical and shorter methods.

2. M. Serret considers, as a generalization of the rectangular hyperbola, curves whose asymptotes meet in a point and are parallel to the sides of a regular polygon. I make use of a somewhat similar, but less restricted, class of curves. In fact, the asymptotes are parallel to the sides of a regular polygon without being concurrent. A slight difference occurs according as the degree of the curve is odd or even. For example, when the degree is 3 the polygon is an equilateral triangle; but when the degree is 4 the polygon is a regular octagon, and not a square; for we require four different directions for the asymptotes. Uniformity is secured by saying that the curve of degree n has its asymptotes parallel to the sides of a regular polygon of m sides, and, for brevity, such a curve will be alluded to as an *isogonal* curve.

3. To discuss such curves we use axes of coordinates OI, OJ, where O is an arbitrary origin and I, J are the circular points at infinity. The equation of n lines through the origin parallel to the sides of a regular polygon of m sides will be of the form

$$x^n = ay^n.$$

---

* *Comptes Rendus*, 1894, 1895.

† *Proc. of the Amer. Math. Soc.*, Vol. I.

And hence the general equation of an isogonal curve of degree n is

$$f \equiv ax^n + by^n + na_1 x^{n-1} + n(n-1) b_1 x^{n-2} y - \dots$$
$$\dots n(n-1) c_1 xy^{n-2} + d_1 y^{n-1} + \dots = 0,$$

the only restrictions being that n coefficients in the general equation vanish. By suitably choosing the origin, *i.e.*, so as to satisfy the equations

$$x + a_1 = 0 \quad \text{or} \quad \frac{\partial^{n-1} f}{\partial x^{n-1}} = 0,$$

$$y + a_1 = 0 \quad \text{or} \quad \frac{\partial^{n-1} f}{\partial y^{n-1}} = 0,$$

the terms in x^{n-1} and y^{n-1} can be made to disappear. On the analogy with conics we are tempted to call this new origin the centre of the curve. As a matter of fact, if we bear in mind that the centre of a curve coincides with the mean centre of the points of intersection of its asymptotes, it can be verified by a short calculation that the point in question is actually the centre in the standard sense introduced by Chasles.

4. By using the equation written above some of the well known properties of rectangular hyperbolas can be extended to all isogonal curves. Thus, if S and S' be two such curves of the n-th degree, then all curves of degree n through their common points are isogonal curves, and the centre locus is a circle. But for our purpose the following theorem is of more importance:—

The first polar of any point at infinity with respect to an isogonal curve of the n-th degree is an isogonal curve of the $(n-1)$-th degree, and the locus of the centres of these curves is a circle concentric with the original curve.

In fact, taking for origin the centre of the curve, we have

$$a_1 = d_1 = 0,$$

and the equation of the first polar of a point at infinity is

$$x_1 \frac{\partial f}{\partial x} + y_1 \frac{\partial f}{\partial y} = 0$$

$$\text{or } x_1 \left\{ ax^{n-1} + (n-1)(n-2) b_1 x^{n-3} y + \dots + (n-1) c_1 z^{n-2} + \dots \right\}$$
$$+ y_1 \left\{ by^{n-1} + (n-1) b_1 x^{n-2} + \dots + (n-1)(n-2) c_1 xy^{n-3} + \dots \right\} = 0,$$

and the centre of this isogonal curve is given by

$$ax_1x+b_1y_1 = 0,$$

$$by_1y+c_1x_1 = 0\,;$$

so that when x_1, y_1 vary the centre locus is the circle whose equation is

$$abxy = b_1c_1.$$

This proves the theorem enunciated above.

5. Consider now three lines whose equations are $P_1 = 0$, $P_2 = 0$, $P_3 = 0$.

Included in $$\lambda_1P_1^2+\lambda_2P_2^2+\lambda_3P_3^2 = 0$$

there is a pencil of isogonal curves, for, in general, $(n-1)$ linear conditions ensure a curve of degree n being isogonal. These curves are, of course, the rectangular hyperbolas self-conjugate with respect to the triangle formed by the three lines, and their centre locus is the circumcircle.

But included in $$\mu_1P_1^3+\mu_2P_2^3+\mu_3P_3^3 = 0$$

there is just one isogonal cubic, and, as all its first polars are of the type

$$\gamma_1P_1^2+\gamma_2P_2^2+\gamma_3P_3^2 = 0,$$

those of the points at infinity must be the rectangular hyperbolas above. Hence, by the theorem of § 4, the centre of the single isogonal cubic is the centre of the circumscribing circle of the triangle.

6. Next consider four lines $P_1 = 0$, $P_2 = 0$, $P_3 = 0$, $P_4 = 0$.

Included in $$\lambda_1P_1^4+\lambda_2P_2^4+\lambda_3P_3^4+\lambda_4P_4^4 = 0$$

there is a single isogonal curve, and the first polars of points at infinity are isogonal curves of the form

$$\mu_1P_1^3+\mu_2P_2^3+\mu_3P_3^3+\mu_4P_4^3 = 0.$$

Now, if we take the first polar of the point at infinity on P_4, we see that $\mu_4 = 0$, and the pencil of polars includes the single isogonal cubic which we have seen to be included in

$$\mu_1P_1^3+\mu_2P_2^3+\mu_3P_3^3 = 0.$$

The centres of all the polars lie on a circle, and, by § 5, this circle passes through the centres of the circumcircles of the four triangles formed by the four lines. Further, its centre is the centre of the isogonal curve included in

$$\lambda_1 P_1^4+\lambda_2 P_2^4+\lambda_3 P_3^4+\lambda_4 P_4^4 = 0.$$

We call this the centre circle of the four lines. Its defining property as here given is well known in elementary geometry.

7. Next consider five lines P_1, P_2, P_3, P_4, P_5.

There is a single isogonal curve included in

$$\lambda_1 P_1^5+\lambda_2 P_2^5+\lambda_3 P_3^5+\lambda_4 P_4^5+\lambda_5 P_5^5 = 0,$$

and among the first polars of points at infinity is the single isogonal quartic defined by any four of the lines. Thus the centre locus is a circle containing the centres of the centre circles obtained from the lines by leaving out each one in turn, and its centre is the centre of the isogonal quintic. We call this the centre circle of the five lines.

8. In just the same way, by considering the isogonal sextic included in

$$\lambda_1 P_1^6+\lambda_2 P_2^6+\ldots+\lambda_6 P_6^6 = 0,$$

we see that the centres of the five centre circles obtained by omitting the lines in turn lie on a circle whose centre is the centre of this sextic, and so on for seven, eight, ... lines *ad inf.*; belonging to n lines we have a circle called the centre circle. Then, taking $(n+1)$ lines, we obtain $(n+1)$ of these circles by omitting each line in turn, and the centres of these $(n+1)$ circles are concyclic.

9. It is easy to see that the $(n+1)$ circles also meet in a point. In fact, take the case of six lines: the centre circle of five lines P_1, P_2, P_3, P_4, P_5 is the locus of the centres of isogonal quartics included in

$$\lambda_1 P_1^4+\lambda_2 P_2^4+\lambda_3 P_3^4+\lambda_4 P_4^4+\lambda_5 P_5^4 = 0, \tag{A}$$

and consequently, when the centre circle belonging to $P_1P_2P_3P_4P_5$ meets that belonging to $P_1P_2P_3P_4P_6$, we have a centre of a quartic S included in (A), and of a quartic S' included in

$$\lambda_1 P_1^4+\lambda_2 P_2^4+\lambda_3 P_3^4+\lambda_4 P_4^4+\lambda_6 P_6^4 = 0.$$

But

$$\kappa S+\kappa' S' = 0$$

will then be an isogonal quartic having its centre at this point for all values of κ and κ', and, by suitably choosing κ and κ', we can make this quartic belong to the set derived from any five of the lines, unless $\lambda_5 = \lambda_6 = 0$. Hence, if a point lies on two of the centre circles, it lies on each of them, unless it be the centre of an isogonal quartic included in

$$\lambda_1 P_1^4+\lambda_2 P_2^4+\lambda_3 P_3^4+\lambda_4 P_4^4 = 0.$$

In the case above the centre circle belonging to $P_1P_2P_3P_4P_5$ meets that belonging to $P_1P_2P_3P_4P_6$ in two points: one is the centre of the unique isogonal quartic included in

$$\lambda_1 P_1^4+\lambda_2 P_2^4+\lambda_3 P_3^4+\lambda_4 P_4^4 = 0,$$

and the other is the common point spoken of above.

10. The greater part of the above reasoning can be put into the language of synthetic geometry without difficulty.

In an isogonal curve the polar line of I always passes through J, and *vice versa*, while the two polars meet in the centre of the curve. For a pencil of isogonal curves corresponding polars form two projective pencils through I and J, and hence the centre locus is a circle.

Applications to Dynamics of some Algebraical Results.

By T. J. I'A. BROMWICH.

Received November 6th, 1900. Communicated November 8th, 1900. Received, in revised form, January 9th, 1901.

The problem considered in this paper is that of the small oscillations of a dynamical system about a state of steady motion. In § 1 the Hamiltonian equations are used to determine the principal coordinates of an oscillation in the neighbourhood of a state of steady motion; the suggestion of using the Hamiltonian function instead of the Lagrangian was made to me by Mr. E. T. Whittaker, and, so far as I know, the results obtained in this way are novel. In § 2 an approximate method for dealing with gyrostatic systems is given; this method has been used by Thomson and Tait, but their work can be abbreviated by using the algebraical results quoted.

It is proved below that the problems in §§ 1, 2 both depend on the algebraic reduction to a canonical shape of two bilinear forms, one being symmetric and the other alternate; this reduction has been carried out in various papers, but these are somewhat lengthy. It seemed, therefore, worth while to indicate briefly a method which (though not exhaustive) will cover many of the cases met with; this method is given in § 3.

1. *Principal Coordinates in Small Oscillations.*

When we have to consider the problem of small oscillations of a dynamical system about a position of equilibrium, it is well known that the determination of the principal (or normal) coordinates depends on the reduction of two quadratic forms to sums of squares; these quadratic forms being the kinetic and potential energies of the system. But, if we are dealing with small oscillations about a state of steady motion, the problem of finding principal coordinates is not so simple; and, if we use the Lagrangian equations of motion, there is apparently no method of solving the problem. For (see Routh's *Advanced Rigid Dynamics* [1892], Art. 111), if we choose the coordinates so as to vanish in the steady motion, the Lagrangian function* can be reduced to the form

$$Q+B+Q',$$

where Q, Q' are quadratic functions of the velocities and coordinates respectively and B is a bilinear function of the two. We must notice that B must *not* be assumed to be a symmetrical bilinear form; for, if so, B would be a perfect differential with respect to the time, and would not affect the equations of motion. On the other hand, B may always be replaced by an alternate bilinear form; this point will be considered later (in § 2). Now it is in general quite impossible to reduce the three forms Q, B, Q' to canonical forms, the velocities and coordinates being, of course, necessarily subject to the same substitutions; and this is why the determination of principal coordinates is, at first sight, impossible. In the case of oscillations about a state of equilibrium, B vanishes identically, for the coefficients of B depend on the velocities of the steady motion and vanish with them; hence, in this case, the difficulty just pointed out does not arise.

But it will be proved that, if we use the Hamiltonian equations of motion, the Hamiltonian function can be reduced to a canonical form; for, in this system, it is not necessary to keep the coordinates and the momenta distinct. That is, we can take as a new coordinate some function both of the coordinates and of the momenta, with a corresponding change in the momenta. It is, of course, necessary that the transformation should be subject to certain conditions in order that the standard Hamiltonian form of the equations of motion may be retained. The conditions on the transformation can be expressed in the following form:—

---

* This is, of course, the first approximation only; we shall, throughout, make the customary assumption that the disturbance from the steady motion is *small*.

Let $(q_1, \ldots, q_n)$, $(p_1, \ldots, p_n)$ be the coordinates and momenta of a system having n degrees of freedom; and let $(q_1', \ldots, q_n')$, $(p_1', \ldots, p_n')$ be the transformed coordinates and momenta. Then, in order that the Hamiltonian equations may remain unchanged in form, we must have equations of the type

$$p_r = \frac{\partial W}{\partial q_r}, \quad q_r' = \frac{\partial W}{\partial p_r'} \quad (r = 1, 2, \ldots, n),$$

where W is a function of $q_1, \ldots, q_n, p_1', \ldots, p_n'$. Other forms of the conditions may be given, say, for instance,

$$p_r = -\frac{\partial U}{\partial q_r}, \quad p_r' = \frac{\partial U}{\partial q_r'} \quad (r = 1, 2, \ldots, n),$$

U being a function of $q_1, \ldots, q_n, q_1', \ldots, q_n'$; and, of course, there is a similar form giving q_r, q_r' in terms of the p's.

We shall now prove that these conditions can be put in another form. Let δ, Δ be any two *commutative* symbols of variation; then

$$\begin{aligned}\delta W &= \Sigma \left(\frac{\partial W}{\partial q_r}\delta q_r + \frac{\partial W}{\partial p_r'}\delta p_r'\right) \\ &= \Sigma\, (p_r \delta q_r + q_r' \delta p_r'),\end{aligned}$$

by our first set of conditions. Hence

$$\Delta \delta W = \Sigma\, (\Delta p_r . \delta q_r + \Delta q_r' . \delta p_r' + p_r . \Delta \delta q_r + q_r' . \Delta \delta p_r').$$

Similarly, $\delta \Delta W = \Sigma\, (\delta p_r . \Delta q_r + \delta q_r' . \Delta p_r' + p_r . \delta \Delta q_r + q_r' . \delta \Delta p_r')$.

Now these two expressions must be the same, and so

$$\Sigma\, (\delta p_r . \Delta q_r - \delta q_r . \Delta p_r) = \Sigma\, (\delta p_r' . \Delta q_r' - \delta q_r' . \Delta p_r').$$

It is readily seen that the other conditions lead to the same result; and it is easy to see the correctness of the condition when written in this shape. For the original Hamiltonian equations are

$$\frac{dq_r}{dt} = \frac{\partial H}{\partial p_r}, \quad \frac{dp_r}{dt} = -\frac{\partial H}{\partial q_r} \quad (r = 1, 2, \ldots, n).$$

Thus
$$\delta H = \Sigma \left(\delta p_r \frac{dq_r}{dt} - \delta q_r \frac{dp_r}{dt}\right)$$
$$= \Sigma \left(\delta p_r' \frac{dq_r'}{dt} - \delta q_r' \frac{dp_r'}{dt}\right),$$

in virtue of the condition just obtained, and so

$$\frac{dq_r'}{dt} = \frac{\partial H}{\partial p_r'}, \quad \frac{dp_r'}{dt} = -\frac{\partial H}{\partial q_r'},$$

or the Hamiltonian equations remain of the same form after the transformation, provided that

$$\Sigma \left(\delta p_r \Delta q_r - \delta q_r \Delta p_r\right)$$

remains unaltered; and it is not necessary (contrary to what might possibly be expected) to alter H except by the substitutions.

We turn now to the consideration of the special problem originally contemplated. In a steady motion all the momenta will be constant, say that they are $a_1, \ldots, a_n$ respectively (of course some of these constants may be zero); some of the coordinates will be constant too, say that $q_1, \ldots, q_k = b_1, \ldots, b_k$ respectively; while the other coordinates will vary uniformly and will not appear in the Hamiltonian function except through their momenta, say that $\frac{dq_{k+1}}{dt}, \ldots, \frac{dq_n}{dt}$ are in the steady motion $c_{k+1}, \ldots, c_n$ respectively. Then let us put

$$p_r = a_r + \xi_r \quad (r = 1, 2, \ldots, n),$$
$$q_r = b_r + x_r \quad (r = 1, 2, \ldots, k),$$
$$\frac{dq_r}{dt} = c_r + \frac{dx_r}{dt} \quad (r = k+1, k+2, \ldots, n),$$

and H will become, on expansion,

$$H_0 + H_1 + H_2 + \ldots,$$

where H_m is a homogeneous function of degree m in the x's and ξ's, the coefficients depending on the a's and b's.

Then, since the steady motion given by the equations

$$x_r = 0, \quad \xi_r = 0$$

is supposed possible, we shall have from the Hamiltonian equations of motion

$$0 = \frac{\partial H_1}{\partial \xi_r} \quad (r = 1, 2, \ldots, k),$$

$$c_r = \frac{\partial H_1}{\partial \xi_r} \quad (r = k+1, k+2, \ldots, n),$$

$$0 = \frac{\partial H_1}{\partial x_r} \quad (r = 1, 2, \ldots, n).$$

Hence H_1 contains only $\xi_{k+1}, \ldots, \xi_n$, and no x's at all. Assuming now that the motion is *slightly* disturbed from the steady state, and never differs much from it, all the x's and ξ's will be small; so that the approximate equations of motion are

$$\frac{dx_r}{dt} = \frac{\partial H_2}{\partial \xi_r}, \quad \frac{d\xi_r}{dt} = -\frac{\partial H_2}{\partial x_r} \quad (r = 1, 2, \ldots, n).$$

So for the problem in hand we can fix our attention on H_2 only, and we can consider H_2 as the Hamiltonian function, the x's and ξ's being treated as the coordinates and momenta respectively—since $q_{k+1}, \ldots, q_n$ appear nowhere in H, $x_{k+1}, \ldots, x_n$ will not appear in H_2; this fact will not, however, affect the algebraic problem.

The problem, then, is to reduce H_2 to a canonical form by linear substitutions on the x's and ξ's, which are such that

$$\Sigma \, (\delta x_r \Delta \xi_r - \delta \xi_r \Delta x_r)$$

remains the same. But, since the substitutions are *linear*, the δx's and $\delta \xi$'s are transformed by the same substitutions as the x's and ξ's, and so, too, the Δx's and $\Delta \xi$'s. Hence our linear substitutions are to be such that

$$\Sigma \, (x_r \eta_r - y_r \xi_r)$$

remains unaltered, where y_r, η_r are any variables which must be transformed by the same substitutions as x_r, ξ_r respectively.

The investigation is now reduced to one covered by previous papers,* namely, the simultaneous reduction of a symmetric and an alternate bilinear form. For we can replace H_2 (a quadratic function of the x's and ξ's) by a bilinear form symmetric in the x's, ξ's and y's, η's; thus, if

$$H_2 = \tfrac{1}{2}\Sigma a_{rs} x_r x_s + \Sigma b_{rs} x_r \xi_s + \tfrac{1}{2}\Sigma c_{rs} \xi_r \xi_s,$$

---

* *Proc. Lond. Math. Soc.*, Vol. xxxii., 1900, p. 321; *Amer. Jour. of Math.*, Vol. xxiii., 1901.

where $$a_{rs} = a_{sr}, \quad b_{rs} \neq b_{sr}, \quad c_{rs} = c_{sr},$$
we consider the equivalent form

$$A = \Sigma a_{rs} x_r y_s + \Sigma b_{rs} (x_r \eta_s + y_r \xi_s) + \Sigma c_{rs} \xi_r \eta_s.$$

Then we have to effect the simultaneous reduction (by congruent substitutions) of A and B, where B is the alternate form

$$\Sigma (x_r \eta_r - y_r \xi_r),$$

and our transformations are to be adjusted so as to leave B unaltered. It will be observed that the determinant

$$| B | = (-1)^m \quad [\text{where } m = n(n+1)]$$
$$= +1;$$

so that three of the six cases considered in the papers quoted do not occur: namely, there are no zero roots of $| \lambda A - B | = 0$ (which accounts for two of the six), and, further, $| \lambda A - B | \not\equiv 0$. For our present purpose it is preferable to write the determinantal equation in the form $| A - \mu B | = 0$, for $| B | \neq 0$, though $| A |$ may be zero. We have then the reduced parts corresponding to—

(i.) A pair of invariant factors $(\mu - c)^e$, $(\mu + c)^e$ $(c \neq 0)$,

$$(A) \qquad c(x_1 \eta_1 + y_1 \xi_1) + \ldots + c(x_e \eta_e + y_e \xi_e)$$
$$+ (x_1 \eta_2 + y_1 \xi_2) + \ldots + (x_{e-1} \eta_e + y_{e-1} \xi_e),$$
$$(B) \qquad (x_1 \eta_1 - y_1 \xi_1) + \ldots + (x_e \eta_e - y_e \xi_e),$$

where we have written ξ_r instead of x_{2e+1-r} $(r = 1, 2, \ldots, e)$ in the notation of my last paper;* this change is, of course, to retain the proper form for B.

(ii.) If $c = 0$ and e be odd, we still have a pair of invariant-factors, and the results are as in (i.).

(iii.) If $c = 0$, and e be *even* $(= 2p)$, we have

$$(A) \quad (x_1 \eta_2 + y_1 \xi_2) + \ldots + (x_{p-1} \eta_p + y_{p-1} \xi_p) + x_p y_p,$$
$$(B) \quad (x_1 \eta_1 - y_1 \xi_1) + \ldots + (x_p \eta_p - y_p \xi_p),$$

where, again, we have changed the notation, writing ξ_r instead of x_{2p+1-r} $(r = 1, 2, \ldots, p)$, in order to retain the form of B.† There are special cases of these results, namely :—

---

* See *Proc. Lond. Math. Soc.*, Vol. XXXII., p. 336; the order of the suffixes is rather different in the paper printed in the *American Journal.*

† *Loc. cit.*, p. 340.

If $e = 1$ and $c \neq 0$, we have the typical terms

$$(A) \quad c\,(x_1\eta_1 + y_1\xi_1),$$

$$(B) \quad x_1\eta_1 - y_1\xi_1,$$

and, if $c = 0$ with $e = 1$, we have a pair of invariant-factors μ, μ, and the typical terms are as in the last case with $c = 0$.

If $c = 0$ and $e = 2$, we have the terms

$$(A) \quad x_1 y_1,$$

$$(B) \quad x_1\eta_1 - y_1\xi_1,$$

and this will be in general the part of the reduced forms corresponding to a coordinate which changes uniformly in the steady motion.

Thus we have the corresponding terms in H_2 :—

(i.) Two invariant-factors $(\mu - c)^e$, $(\mu - c)^e$ $(c \neq 0)$,

$$c\,(x_1\xi_1 + \ldots + x_e\xi_e) + (x_1\xi_2 + \ldots + x_{e-1}\xi_e),$$

and, if $e = 1$, we have simply

$$cx_1\xi_1.$$

(ii.) Two invariant-factors μ^e, μ^e (*e odd*) give the same as (i.), but with $c = 0$.

(iii.) One invariant-factor μ^{2p},

$$(x_1\xi_2 + \ldots + x_{p-1}\xi_p) + \tfrac{1}{2}x_p^2,$$

and, if $p = 1$, we have $\qquad \tfrac{1}{2}x_1^2.$

The invariant-factors just referred to are those of the determinant $| A - \mu B |$, which is, when written out at full length,

$$\begin{vmatrix} a_{11}, & a_{12}, & \ldots, & a_{1n}, & b_{11} - \mu, & b_{12}, & \ldots, & b_{1n} \\ a_{21}, & a_{22}, & \ldots, & a_{2n}, & b_{21}, & b_{22} - \mu, & \ldots, & b_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1}, & a_{n2}, & \ldots, & a_{nn}, & b_{n1}, & b_{n2}, & \ldots, & b_{nn} - \mu \\ b_{11} + \mu, & b_{21}, & \ldots, & b_{n1}, & c_{11}, & c_{12}, & \ldots, & c_{1n} \\ b_{12}, & b_{22} + \mu, & \ldots, & b_{n2}, & c_{21}, & c_{22}, & \ldots, & c_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ b_{1n}, & b_{2n}, & \ldots, & b_{nn} + \mu, & c_{n1}, & c_{n2}, & \ldots, & c_{nn} \end{vmatrix}.$$

Here the a's, b's, c's are the coefficients in the quadratic form H_2, and are defined by

$$2H_2 = \Sigma\, a_{rs} x_r x_s + 2\Sigma\, b_{rs} x_r \xi_s + \Sigma\, c_{rs} \xi_r \xi_s.$$

It may be well to point out that, as proved by Kronecker,* the invariant-factors of the type μ^{2p+1} always occur in pairs, while those of the type μ^{2p} may appear singly. Of course, if $c \neq 0$, we always have pairs $(\mu - c)^e$, $(\mu + c)^e$ whatever e may be.

A simple method of reducing A and B applicable when the invariant-factors are linear is indicated in § 3 below.

The Hamiltonian equations of motion

$$\frac{dx_r}{dt} = \frac{\partial H_2}{\partial \xi_r}, \quad \frac{d\xi_r}{dt} = -\frac{\partial H_2}{\partial x_r}$$

will now take various forms corresponding to the different types of invariant-factors. Thus we have:—

(i.) Invariant-factors $(\mu - c)^e$, $(\mu + c)^e$, and $c \neq 0$,

$$\begin{array}{ll} \dfrac{dx_1}{dt} = cx_1, & \dfrac{d\xi_1}{dt} = -(c\xi_1 + \xi_2), \\[2ex] \dfrac{dx_2}{dt} = cx_2 + x_1, & \dfrac{d\xi_2}{dt} = -(c\xi_2 + \xi_3), \\[2ex] \ldots \quad \ldots \quad \ldots & \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\[2ex] \dfrac{dx_e}{dt} = cx_e + x_{e-1}, & \dfrac{d\xi_e}{dt} = -c\xi_e. \end{array}$$

These give
$$\left.\begin{array}{r} x_r = \left[A_1 \dfrac{t^{r-1}}{(r-1)!} + A_2 \dfrac{t^{r-2}}{(r-2)!} + \ldots + A_r\right] \exp(ct) \\[2ex] (-1)^{r-1} \xi_{e+1-r} = \left[B_1 \dfrac{t^{r-1}}{(r-1)!} + B_2 \dfrac{t^{r-2}}{(r-2)!} + \ldots + B_r\right] \exp(-ct) \end{array}\right\}$$
$$(r = 1, 2, \ldots, e).$$

In particular, if $e = 1$, we have

$$x_1 = A \exp(ct), \quad \xi_1 = B \exp(-ct).$$

(ii.) If $c = 0$ and e is odd, we get the same results as in case (i.) with c put zero.

---

[*] *Berliner Monatsberichte*, 1874, p. 441; *Gesammelte Werke*, Bd. I., p. 477; see [illegible] Stickelberger, *Crelle*, Bd. LXXXVI., 1879, p. 20, § 5, and Muth's *Elementartheiler*, [illegible]140.

(iii.) If $c = 0$ and $e = 2p$, we find

$$\frac{dx_1}{dt} = 0, \qquad \frac{d\xi_1}{dt} = -\xi_2,$$

$$\frac{dx_2}{dt} = x_1, \qquad \frac{d\xi_2}{dt} = -\xi_3,$$

$$\ldots \quad \ldots \qquad \ldots \quad \ldots$$

$$\frac{dx_p}{dt} = x_{p-1}, \qquad \frac{d\xi_p}{dt} = -x_p.$$

Then $$x_r = A_1\frac{t^{r-1}}{(r-1)!} + A_2\frac{t^{r-2}}{(r-2)!} + \ldots + A_r \quad (r = 1, 2, \ldots, p),$$

$$(-1)^{r-p}\xi_{2p+1-r} = A_1\frac{t^{r-1}}{(r-1)!} + A_2\frac{t^{r-2}}{(r-2)!} + \ldots + A_r$$
$$(r = p+1,\ p+2,\ \ldots,\ 2p).$$

In particular, if $e = 2$ or $p = 1$,

$$x_1 = A, \quad \xi_1 = -(At+B).$$

From these results it follows that, if the coordinates are to contain only periodic functions of the time, all the quantities c must be pure imaginaries and all the indices e must be unity. Weierstrass[*] has shown that a *sufficient* condition for this is that H_2 should be positive for all real (non-zero) values of the x's and ξ's; it is easy to see, by taking special cases, that this condition is not necessary.[†] Weierstrass's investigation starts from the $2n$ differential equations

$$\frac{dx_r}{dt} = \frac{\partial H}{\partial \xi_r}, \quad \frac{d\xi_r}{dt} = -\frac{\partial H}{\partial x_r} \quad (r = 1, 2, \ldots, n);$$

but he does not reduce the quadratic H_2 to a canonical form; the suggestion of making this reduction is due, I believe, to Mr. E. T. Whittaker, who proposed it to me as an algebraical problem.

It is clear, however, that, if some of the values of c are zero, the coordinates cannot be expressed entirely by means of periodic terms. This will usually be the case if the disturbance is such as to alter the momenta corresponding to those velocities which vary uniformly in the steady motion. Thus, if x_n is a coordinate of this type, we know that

---

[*] *Berliner Monatsberichte*, 1879, p. 430; *cf.* Taber, *Proc. Lond. Math. Soc.*, Vol. xxii., 1891, p. 449, and the author, Vol. xxxii., 1900, p. 92.

[†] An example is worked out by the author (*loc. cit.*, p. 98).

$$\frac{\partial H}{\partial x_n} = 0$$

(see above, p. 201), and hence

$$\frac{d\xi_n}{dt} = 0;$$

or, if in the disturbance from the steady motion ξ_n be altered, that alteration will persist in the subsequent motion. To illustrate the point, let us take the simple case of a particle describing a circle of radius a under a central force varying as r^n.

Here we have, using ordinary plane polars, for the Lagrangian function L,

$$2L = \dot{r}^2 + r^2\dot{\theta}^2 - kr^{n+1},$$

and so, for the Hamiltonian function,

$$\dot{r} = p_1, \quad r^2\dot{\theta} = p_2,$$

and $$2H = p_1^2 + \frac{1}{r^2}p_2^2 + kr^{n+1}.$$

In the steady motion we have

$$r = a, \quad p_1 = 0, \quad p_2 = \text{const.} = b, \text{ say};$$

so write, in general,

$$r = a + x, \quad p_1 = \xi, \quad p_2 = b + \eta.$$

Thus $$2H = \xi^2 + \left(\frac{b+\eta}{a+x}\right)^2 + k\,(a+x)^{n+1},$$

and expanding, as far as the quadratic terms, we find

$$\frac{b^2}{a^2} + ka^{n+1} + \left[(n+1)\,ka^n - \frac{2b^2}{a^3}\right]x + \frac{2b}{a^2}\eta$$
$$+\xi^2 + \left[\frac{3b^2}{a^4} + \frac{n\,(n+1)}{2}ka^{n-1}\right]x^2 - \frac{4b}{a^3}x\eta + \frac{1}{a^2}\eta^2.$$

That the steady motion may exist the coefficient of x must vanish, or

$$(n+1)ka^n - \frac{2b^2}{a^3} = 0.$$

The coefficient of η gives $\frac{b}{a^2}$ for the value of $\dot{\theta}$ in the steady motion, which is, of course, obvious from first principles.

Hence, we have for H_2, the following result, after substituting for k in terms of b^2,

$$2H_2 = \xi^2 + (n+3)\frac{b^2}{a^4}x^2 - \frac{4b}{a^3}x\eta + \frac{1}{a^2}\eta^2$$

$$= \xi^2 + (n+3)\frac{b^2}{a^4}\left(x - \frac{2a\eta}{(n+3)b}\right)^2 + \frac{n-1}{n+3}\,\frac{\eta^2}{a^2}.$$

If now we write

$$X = x - \frac{2a\eta}{(n+3)\,b}, \quad Y = y - \frac{2a\xi}{(n+3)\,b},$$

we find that

$$x\xi' - x'\xi + y\eta' - y'\eta = X\xi' - X'\xi + Y\eta' - Y'\eta$$

(the accented letters being subject to the same substitutions as the unaccented); so that (X, Y), (ξ, η) may be taken as coordinates and momenta respectively.* Then

$$2H_2 = \xi^2 + (n+3)\frac{b^2}{a^4}X^2 + \frac{n-1}{n+3}\,\frac{\eta^2}{a^2},$$

which can be reduced to the canonical form already given; † but it is quite easy to solve the differential equations directly. Thus,

$$\frac{dX}{dt} = \xi, \qquad \frac{d\xi}{dt} = -(n+3)\frac{b^2}{a^4}X,$$

$$\frac{dY}{dt} = \frac{n-1}{n+3}\,\frac{\eta}{a^2}, \qquad \frac{d\eta}{dt} = 0.$$

Hence we have

$$\left.\begin{aligned} X &= X_0 \cos pt + \frac{1}{p}\left(\frac{dX}{dt}\right)_0 \sin pt \\ \xi &= -pX_0 \sin pt + \left(\frac{dX}{dt}\right)_0 \cos pt \end{aligned}\right\} \quad p^2 = (n+3)\frac{b^2}{a^4},$$

---

* It is easy to see that the substitutions above can be derived from

$$\xi = \frac{\partial W}{\partial x}, \quad \eta = \frac{\partial W}{\partial y}, \quad X = \frac{\partial W}{\partial \Xi}, \quad Y = \frac{\partial W}{\partial \mathrm{H}}$$

if

$$W = x\Xi + y\mathrm{H} - \frac{2a\Xi\mathrm{H}}{(n+3)\,b}.$$

† A substitution $X_1 = lX + m\xi$, $\xi_1 = l'X + m'\xi$, will give $X_1\xi_1' - X_1'\xi_1 = X\xi' - X'\xi$, provided that $lm' - l'm = 1$; and it is not difficult to choose l, m, l', m' to satisfy this condition and to give also

$$\xi^2 + (n+3)\frac{b^2}{a^4}X^2 = cX_1\xi_1.$$

$$Y = Y_0 + \frac{n-1}{n+3}\,\frac{1}{a^2}\,(vt),$$

$$\eta = \eta_0.$$

For the sake of example, let us assume that the initial disturbance is such that the particle is not displaced, but has its velocity changed by the small amounts u, v radially and tangentially. Then

$$\left(\frac{dX}{dt}\right)_0 = \left(\frac{dx}{dt}\right)_0 = u = \xi_0,$$

$$X_0 = -\frac{2a\eta_0}{(n+3)\,b} = -\frac{2a^2v}{(n+3)\,b},$$

$$Y_0 = -\frac{2a\xi_0}{(n+3)\,b} = -\frac{2au}{(n+3)\,b}.$$

Hence, we find at time t

$$r = a + x = a + X + \frac{2a}{(n+3)\,b}\,\eta = a + \frac{2a^2v}{(n+3)\,b}\,(1-\cos pt) + \frac{u}{p}\sin pt,$$

$$\theta = \frac{bt}{a^2} + y = \frac{bt}{a^2} + Y + \frac{2a}{(n+3)\,b}\,\xi$$

$$= \left(\frac{b}{a^2} + \frac{n-1}{n+3}\,\frac{v}{a}\right)t - \frac{2au}{(n+3)\,b}\,(1-\cos pt) + \frac{4v}{(n+3)\,a}\,\frac{1}{p}\sin pt.$$

These results can be verified without much difficulty directly from the ordinary polar equations of motion; they show that, if the disturbance is perfectly general, the value of y contains a term which increases with the time, and that the mean value of x is not zero. Thus, speaking strictly, the disturbed motion will, in the course of time, deviate largely from the original steady motion; this does not, of course, vitiate our approximation (provided p be real), for its accuracy depends on the smallness of $\frac{dy}{dt}$, not of y. But, if p be not real, the method of small oscillations cannot be applied at all; and, to determine the stability or instability of the steady motion, we must have recourse to the exact equations of motion.*

---

* The fact that these cases (commonly called unstable) may require further investigation is well illustrated by Prof. Klein's results in the case of the "sleeping" top (*American Bulletin of Math.*, 1896; Klein and Sommerfeld's *Theorie des Kreisels*, Kap. v., §§ 4–8, pp. 316–374). Thus, the method of small oscillations leads to certain condition for stability which may be expressed in the form $k > 0$, where k ds on the constants of the top. Now Klein proves virtually that, for *small* s of k, the sign of k does not affect the *practical* stability; so that there can be no

It is not difficult to see that in general, if q be a coordinate which varies with uniform velocity c in the steady motion, then in a motion arising from a slight disturbance of the steady motion q will contain terms of the type $(c+v)\,t$, where v involves the initial change in p (p being the momentum corresponding to q): this fact may also be illustrated by the nutations of a top about a steady precessional motion (Klein and Sommerfeld, pp. 276, 291). For, since (as already explained, p. 201, above) q does not appear explicitly in the Hamiltonian function, we have the equation

$$\frac{dp}{dt} = 0,$$

or p has the value which it receives just after the disturbance has been applied. Now

$$\frac{dq}{dt} = \frac{\partial H}{\partial p},$$

and, as a rule, $\dfrac{\partial H}{\partial p}$ will contain a term depending on p; so that we may write

$$\frac{dq}{dt} = c+v+\text{terms involving the disturbances of the other coordinates and momenta},$$

where c is the value of $\dfrac{\partial H}{\partial p}$ in the steady motion, and v is proportional to the change in p produced by the disturbance. Thus q will contain a term $(c+v)\,t$, as already stated.

2. *Small Oscillations in Gyrostatic Systems.*

The solution obtained in § 1 for the problem of small oscillations about a state of steady motion, although quite general, may yet in some cases be not so easy of application as the following approximate method, which is based on the Lagrangian equations. The method is suggested by a consideration of Thomson and Tait's results for problems of "gyrostatic domination" (*Natural Philosophy*, §§ 344, 345); in these cases it usually happens that the angular momenta of the gyrostats are large in comparison with the other dynamical constants of the system. It appears to be easier to follow out the consequences of this fact by using the Lagrangian equation of motion, having

---

abrupt change from stability to instability, as k changes from positive to negative. I have proved that the same point occurs in the screw-motion of a solid of revolution through a liquid. (See a paper accepted by the Society at the April meeting.)

"ignored" those coordinates which define the rotations of the gyrostats. If $x_1, \ldots, x_n$ be the remaining coordinates, chosen so as to vanish in the state of steady motion from which the system is disturbed, then, assuming that the x's remain small, the Lagrangian function L can be reduced to the form

$$L = Q + B + Q'$$

to the first approximation, where

$$Q = \tfrac{1}{2}\Sigma a_{rs}\dot{x}_r\dot{x}_s \quad (a_{rs} = a_{sr})$$

is a quadratic function of $\dot{x}_1, \ldots, \dot{x}_n$,

$$B = \Sigma b_{rs}x_r\dot{x}_s \quad (b_{rs} \neq b_{sr})$$

is bilinear in $\dot{x}_1, \ldots, \dot{x}_n$ and $x_1 \ldots x_n$, and

$$Q' = \tfrac{1}{2}\Sigma c_{rs}x_r x_s \quad (c_{rs} = c_{sr})$$

is a quadratic function of $x_1, \ldots, x_n$.

The typical Lagrangian equation of motion is

$$\frac{d}{dt}\left(\frac{\partial L}{\partial \dot{x}_r}\right) - \frac{\partial L}{\partial x_r} = 0,$$

or $$\frac{d}{dt}(\Sigma a_{rs}\dot{x}_s + \Sigma b_{sr}x_s) - (\Sigma b_{rs}\dot{x}_s + \Sigma c_{rs}x_s) = 0,$$

or $$\Sigma a_{rs}\ddot{x}_s + \Sigma (b_{sr} - b_{rs})\,\dot{x}_s - \Sigma c_{rs}x_s = 0.$$

Thus the coefficients of B appear only in the form $(b_{sr} - b_{rs})$; and we shall not affect the equations of motion by taking instead of B the alternate form

$$\Sigma \tfrac{1}{2}(b_{rs} - b_{sr})\,x_r\dot{x}_s = \Sigma b'_{rs}x_r\dot{x}_s,$$

for we have $b'_{sr} - b'_{rs} = \tfrac{1}{2}(b_{sr} - b_{rs}) - \tfrac{1}{2}(b_{rs} - b_{sr}) = b_{sr} - b_{rs}$.

Another way of obtaining this fact is by subtracting from the Lagrangian function the perfect differential with respect to the time,

$$\frac{d}{dt}\Sigma \tfrac{1}{4}(b_{rs} + b_{sr})\,x_r x_s = \Sigma \tfrac{1}{2}(b_{rs} + b_{sr})\,x_r\dot{x}_s;$$

for it is known that the addition or subtraction of such a perfect differential will not alter the equations of motion.

It will thus be convenient to alter the notation slightly, and, for the future, we shall drop the accents from the alternate form $\Sigma b'_{rs}x_r\dot{x}_s$, and write for it

$$B = \Sigma b_{rs}x_r\dot{x}_s \quad (\text{where } b_{rs} = -b_{sr}).$$

It is of importance now to see under what conditions the coefficients in B are large compared with those in Q, Q'; to make this clear, consider *a single gyrostat* with moment of inertia I and angular velocity

ω. Then one term in the kinetic energy is

$$\tfrac{1}{2}I\omega^2 = \tfrac{1}{2}I(\dot{\phi}+\chi)^2,$$

where ϕ gives the angular position of the gyrostat with respect to some frame in which the axis of the gyrostat is fixed and χ will be the angular velocity of the frame about the axis of the gyrostat; so that χ is some linear function of the velocities, the coefficients involving the coordinates. We assume that ϕ appears in no other way in the Lagrangian function, and then, "ignoring" ϕ, we find the term for Routh's modified function

$$I\omega\chi - \tfrac{1}{2}I\omega^2.$$

The term $(-\tfrac{1}{2}I\omega^2)$ does not contribute to the equations of motion (assuming that the disturbance from the steady motion is not such as to alter ω). Thus χ must be calculated accurately to terms of the second order in $x_1, \ldots, x_n, \dot{x}_1, \ldots, \dot{x}_n$; if there is no initial steady motion except the spins of the gyrostats, χ will be of the form

$$\Sigma f_r \dot{x}_r + \Sigma g_{rs} x_r \dot{x}_s \quad (g_{rs} \neq g_{sr}),$$

and thus the first sum $(\Sigma f_r \dot{x}_r)$ will not affect the equations of motion, or the whole effective contribution to L from this gyrostat will be

$$I\omega\,(\Sigma g_{rs} x_r \dot{x}_s),$$

which will, accordingly, form part of B. Now, by our hypothesis, the angular momenta, such as $I\omega$, of all the gyrostats are large in comparison with the other dynamical constants of the system; hence the coefficients of B are large in comparison with those of Q and Q' in L.

On the other hand, if in the steady motion any coordinates other than the gyrostatic ones vary uniformly, χ will, in general, contain also terms of the type

$$\Sigma h_r x_r + \Sigma k_{rs} x_r x_s.$$

Thus the terms $I\omega(\Sigma h_r x_r)$ in the Lagrangian function will have to be balanced by other terms from the potential energy, so that its coefficients are of the same order as $I\omega$, and, besides this, the terms $I\omega(\Sigma k_{rs} x_r x_s)$ must be included in Q'; then it does not follow that the coefficients of B are necessarily large in comparison with those of Q'.*

---

* To illustrate this point we may consider a top (with moments of inertia A, C) spinning about a point on its axis with angular velocity ω, taking for simplicity the case of no forces. If there is a steady motion in which the axis of the top describes a cone of semi-vertical angle α, the effective terms in the Lagrangian function can be reduced to $\tfrac{1}{2}[A(\dot{x}^2+\dot{y}^2) + 2C\omega x\dot{y} - (C\omega \tan\alpha)^2 x^2/A]$. But, if the axis of the top is originally in a fixed direction, we may simply put $\alpha = 0$, and then the terms are

$$\tfrac{1}{2}A(\dot{x}^2+\dot{y}^2) + C\omega x\dot{y}.$$

In the following work we make the hypothesis that the coefficients of B are large compared with those of Q and Q'; thus it will be only applicable in general if the original steady motion is confined to the gyrostatic spins, though there may be special cases to which the work applies even when there is a further steady motion.

Now consider, first, Q and B simultaneously; and, second, Q' and B simultaneously. Each pair can be reduced to a canonical form by known results by considering the equivalent problems of handling

(i.) The two bilinear forms

$$A = \Sigma a_{rs} x_r y_s \quad \text{(symmetrical)},$$

$$B = \Sigma b_{rs} x_r y_s \quad \text{(alternate)};$$

and (ii.) the two bilinear forms

$$C = \Sigma c_{rs} x_r y_s \quad \text{(symmetrical)},$$

$$B = \Sigma b_{rs} x_r y_s \quad \text{(alternate)},$$

the substitutions being in each case congruent. Since Q is the value of the kinetic energy when the gyrostats have no spins, it follows that Q is essentially positive; thus Weierstrass's theorem* can be applied to show that all the invariant factors of the fundamental determinant $|\lambda A - B|$ are linear and that all the roots of $|\lambda A - B| = 0$ are imaginary. It is then easy to see that we can reduce Q and B by *real* transformations to the forms†

$$Q = \tfrac{1}{2}\Sigma\,(\dot{x}_{2r}^2 + \dot{x}_{2r+1}^2),$$

$$B = \Sigma a_r\,(x_{2r}\dot{x}_{2r+1} - x_{2r+1}\dot{x}_{2r}),$$

where $(\lambda^2 + a_r^2)$ is a typical factor of $|\lambda A - B|$. The form of Q' will not, as a rule, be reduced at all by these substitutions; and the equations of motion become

$$\ddot{x}_{2r} - 2a_r\dot{x}_{2r+1} = \Sigma c_{2r,s} x_s,$$

$$\ddot{x}_{2r+1} + 2a_r\dot{x}_{2r} = \Sigma c_{2r+1,s} x_s.$$

Now, assuming that the a's are large compared with the c's, which will usually follow from our hypothesis regarding the coefficients of B

---

[*] See § 1 above, p. 205; another (and more elementary) proof that the roots of $|\lambda A - B| = 0$ are pure imaginaries is given by Prof. Elliott (*Quart. Jour. of Math.*, December, 1899), though the fundamental point of the proof is the same as that of *those* quoted before.

[†] *See § 3 below, and the papers referred to in § 1.*

and Q', these equations give as an *approximate* solution

$$x_{2r} = A_r \sin(2a_r t + \kappa_r),$$

$$x_{2r+1} = A_r \cos(2a_r t + \kappa_r),$$

and we can proceed to further approximations by substituting these values for the x's on the right-hand side of the equations last found. It follows that we can obtain a first approximation to some of the periods (namely, π/a_r) and the corresponding principal coordinates by neglecting Q' and simply considering the Lagrangian function as $Q+B$. In almost exactly the same way we can show that a first approximation to the remaining periods and coordinates can be found by taking the Lagrangian function as $B+Q'$, rejecting Q. We find that, if $(\lambda^2+\beta^2)$ is a typical factor of the determinant $|\lambda C - B|$, then the corresponding period is nearly $4\pi\beta$. The first set of oscillations will be extremely rapid and the second set extremely slow. It is of some importance to observe that our argument proving that the roots of $|\lambda A - B| = 0$ are pure imaginaries can only be applied to the second set of periods (*i.e.*, those given by $|\lambda C - B| = 0$) if Q' be definite as well as Q; and this point may be of importance in deciding the stability of the system; it is clear from what we have said that the instability, if it exists, will arise from the vibrations of long period. A special case illustrating this is given by Thomson and Tait (*Natural Philosophy*, § 345^{x}), taking the case represented by

$$2L = \dot{x}^2 + \dot{y}^2 + N(x\dot{y} - \dot{x}y) + ax^2 + by^2,$$

and it is proved that the system is only certainly stable if ab is positive, which is precisely the condition that (ax^2+by^2) should be always of one sign, or *definite*.

The condition that Q' should be definite is certainly *sufficient* in all cases to ensure stability, though we have no information as to its necessity; it is, perhaps, worth remarking that the sign of Q' may be either positive or negative, provided that it is always the same. When there are no gyrostatic spins, Q' must be negative for stability.

Finally, it may happen that $|B| = 0$, which will always be the case if n be odd; then there will be certain terms in the reduced form of Q which have no corresponding terms in the reduced form of B. Suppose that the terms $Q_0 = \frac{1}{2}(\dot{x}_1^2 + \ldots + \dot{x}_k^2)$ belong to Q, but that $\dot{x}_1, \ldots, \dot{x}_k$ no not appear in B; we make the necessary substitutions (found in the reducing process) in Q', and then put zero for $x_{k+1}, \ldots, x_n$; we obtain thus a quadratic Q_0' in $x_1, \ldots, x_k$. The terms Q_0, Q_0' can now be reduced simultaneously to sums of squares;* thus we may write

$$Q_0 = \tfrac{1}{2}(\dot{x}_1^2 + \ldots + \dot{x}_k^2),$$

$$Q_0' = -\tfrac{1}{2}(d_1 x_1^2 + \ldots + d_k x_k^2),$$

where these x's are not the same as the last x's, but accents have been dropped to save complicated symbols. Thus the complete expressions are

$$Q = \tfrac{1}{2}(\dot{x}_1^2 + \ldots + \dot{x}_n^2),$$

$$Q' = -\tfrac{1}{2}(d_1 x_1^2 + \ldots + d_k x_k^2) + Q_1',$$

where every term in Q_1' has one of the variables $x_{k+1}, \ldots, x_n$ as a factor. Thus we get k equations of the type

$$\ddot{x}_r = -d_r x_r + (g_{r,k+1} x_{k+1} + \ldots + g_{rn} x_n) \quad (r = 1, 2, \ldots, k)$$

giving k additional periods (neither very long nor very short) of the approximate values $2\pi d_r^{-\frac{1}{2}}$.

3. *A Modified Process of Reduction.*

Let A be a given symmetrical form and B a given alternate form It is required to reduce the two forms by congruent substitutions If we know that all the invariant-factors of the determinan $|\lambda A + \mu B|$ are linear, the method due to Kronecker† takes a simple form, and I venture to give a short sketch of this process, hoping that it may be of interest to some readers who would not study a purely algebraical paper, such as those which I have quoted before The case considered here may be regarded as the ordinary one; for if two forms are chosen at random (one being symmetrical and the other alternate), it will usually happen that all the roots of the determinantal equation $|A - \mu B| = 0$ are different, which is a specia case of linear invariant factors.

Suppose, then, that $\mu = c$ is a root of $|A - \mu B| = 0$; then $(A - cB)$ is a form which can be expressed in terms of (at most) $(n-1)$ x's and $(n-1)$ y's, supposing that the general form $(A - \mu B)$ contains n x's and n y's. Hence, if we are restricted to substitutions which are the same for the x's as the y's, there will be at least one x (and one y) in $(A - cB$ without a corresponding $y(x)$.‡ Let us denote the x by x_1 and the

---

* Weierstrass, *Berliner Monatsberichte*, 1858, p. 207; *Gesammelte Werke*, Bd. I. p. 233; Kronecker, *ibid.*, 1868, p. 339; *Gesammelte Werke*, Bd. I., p. 163.

† *Berliner Monatsberichte*, 1874, p. 397; *Gesammelte Werke*, Bd. I., p. 423.

‡ The case when the $(n-1)$ x's are paired off, each to one of the $(n-1)$ y's, can *occur only when* A, B are expressible in terms of fewer than n x's and n y's.

y by y_2; then we assume that the coefficient of x_1y_2 in $(A-cB)$ is not zero.[*] This assumption is really no more than the original one that the invariant-factors to base $(\mu-c)$ of $|A-\mu B|$ are *linear;* though a direct proof that the two assumptions are equivalent is not to be obtained without going to greater detail than I wish to use here. Thus, the factor multiplying x_1 in $(A-cB)$ is a linear function of $y_2, y_3, \ldots, y_n$; so write y_2' for this factor, and we can eliminate y_2 in terms of $y_2', y_3, \ldots, y_n$. Thus,

$$A-cB = x_1y_2' + \text{terms containing } x_3, x_4, \ldots, x_n \text{ and } y_2', y_3, \ldots, y_n,$$

and, collecting all the terms in y_2', we may write them in the form $x_1'y_2'$, where x_1' is a linear function of $x_1, x_3, \ldots, x_n$. Thus,

$$A-cB = x_1'y_2' + \text{terms in } x_3, \ldots, x_n \text{ and } y_3, \ldots, y_n;$$

then interchange the x's and y's, and we get

$$A+cB = x_2'y_1' + \text{terms of the same type.}$$

Hence $$A = \tfrac{1}{2}(x_1'y_2' + x_2'y_1') + \text{terms in } x_3, \ldots, x_n \text{ and } y_3, \ldots, y_n;$$

$$cB = \tfrac{1}{2}(x_2'y_1' - x_2'y_1') + \text{terms in } x_3, \ldots, x_n \text{ and } y_3, \ldots, y_n.$$

From this result it is clear that $|A-\mu B|$ has two invariant-factors $(\mu-c)$, $(\mu+c)$, which verifies our original assumption partially. It does not, of course, show that, with these invariant-factors, we can have no other forms. Continuing this method, we finally arrive at completely reduced forms for A, B, except for terms which arise when $|A| = 0$ and when $|B| = 0$. The complete discussion of these cases would occupy us too long; but we can indicate how to deal with the simpler points. First take $|B| = 0$; then B can be reduced so as not to contain at least one pair of the variables which are present in A. Say these are x_1, y_1; then, by collecting all the terms in x_1, y_1 together in A, we find (provided the coefficient of x_1y_1 in A does not vanish)[†]

$$A = x_1'y_1' + \text{terms which do not contain } x_1 \text{ or } y_1.$$

---

[*] It may be well to indicate that this is an assumption by giving a case in which it does not hold. Say we take

$$A = c(x_1y_4 + x_2y_3 + x_3y_2 + x_4y_1) + x_3y_4 + x_4y_3,$$
$$B = (x_2y_3 + x_4y_1) - (x_3y_2 + x_1y_4);$$

then $(A-cB)$ contains only x_1, x_3, x_4 and y_2, y_3, y_4; but the term x_1y_2 does not occur.

[†] To illustrate the possibility that this coefficient may vanish, we may take the pair of forms $A = x_1y_3 + x_2y_2 + x_3y_1$, $B = x_2y_3 - x_3y_2$.

The consideration of this case will not be continued here. (Those who are interested in it will find details in my paper in the *American Journal of Mathematics.*)

Thus, we may take x_1', y_1' as new variables in place of x_1, y_1; and these will not appear in B; so that $| \lambda A - B |$ has an invariant-factor λ.

We can in a similar way treat the case $| A | = 0$, and we shall find (in the simplest cases) terms of the type

$$B = x_1' y_2' - x_2' y_1' + \text{terms without these four variables},$$

and either

$$A = x_1' y_1' + \text{terms without these four variables}$$

or $$A = \text{terms without } x_1',\ y_1',\ x_2',\ y_2'.$$

In the first case $| A - \mu B |$ has an invariant-factor μ^2, and in the second it has a pair μ, μ.

It is, perhaps, worth while to indicate the passage from our results to those used in § 2 for the special case when the roots of $| A - \mu B | = 0$ are pure imaginaries. In this case we change $+c$ to $-c$ by changing $+i$ to $-i$, and so $(A - cB)$ to $(A + cB)$. Hence, x_1', x_2' are conjugate imaginaries; for we have

$$A - cB = x_1' y_2' + \text{terms independent of } x_1',\ y_1',\ x_2',\ y_2',$$

$$A + cB = x_2' y_1' + \text{terms independent of } x_1',\ y_1',\ x_2',\ y_2'.$$

Thus, if we write

$$x_1' = \xi_1 + i\xi_2, \quad y_1' = \eta_1 + i\eta_2,$$

$$x_2' = \xi_1 - i\xi_2, \quad y_2' = \eta_1 - i\eta_2,$$

we have, if $c = ia$,

$$A = \xi_1\eta_1 + \xi_2\eta_2 + \text{terms independent of } \xi_1,\ \eta_1,\ \xi_2,\ \eta_2,$$

$$aB = \xi_1\eta_2 - \xi_2\eta_1 + \text{terms independent of } \xi_1,\ \eta_1,\ \xi_2,\ \eta_2,$$

which are the forms used above.

It may be remarked that, in the case of linear invariant-factors, Jordan's methods * can be applied correctly; though, as shown by Kronecker, † they are not sufficient in some other cases. The justice of Kronecker's criticism was (after some controversy) admitted by Jordan, ‡ who adds the remark that his methods are correct in case the symmetric form is equivalent to a *definite* quadratic form. They are valid in all cases when the invariant-factors are linear, even if the quadratic be not definite.

---

* *Liouville's Journal*, t. XIX., 2me sér., 1874, p. 35 (§§ 5–8).

† *Berliner Monatsberichte*, 16 May, 1874, p. 223; *Gesammelte Werke*, Bd. I., p. 402.

‡ *Comptes Rendus*, t. XCII., 1881, p. 1437.

Thursday, December 13th, 1900.

Dr. HOBSON, F.R.S., President, in the Chair.

Sixteen members present.

The following gentlemen were elected members:—Schuyler Colfax Davisson, Ph.D. Tübingen, Associate Professor of University of Indiana; Raghunath Purushottam Paranjpye, B.A. St. John's College, Cambridge; Sidney Luxton Loney, M.A. Sidney Sussex College, Cambridge, Professor of Mathematics at the Royal Holloway College for Women; David Andrew Rothrock, A.B., A.M., Ph.D. Leipsic, Associate Professor of University of Indiana; Balak Ram, B.A., Scholar of St. John's College, Cambridge.

Mr. Basset spoke "On the Real Points of Inflexion of a Curve."

Miss Barwell read a paper entitled "On the Conformal Representation of Polygons on a Half Plane."

Prof. Elliott communicated his paper "On the Syzygetic Theory of Orthogonal Binariants," and gave an account of a paper by Mr. A. L. Dixon, entitled "An Addition Theorem for Hyper-elliptic Functions."

The following papers were communicated by reading their titles:—

On some Properties of Groups of Odd Order (ii.): by Prof. Burnside.

On Discriminants and Envelopes of Surfaces: by Mr. R. W. H. T. Hudson.

Note on the Inflexion of Curves with Double Points: by Mr. H. W. Richmond.

The following presents were made to the Library:—

"Educational Times," December, 1900.

"Indian Engineering," Vol. xxviii., Nos. 16–20, Oct. 20–Nov. 17, 1900.

"Supplemento al Periodico di Matematica," Anno iv., Fasc. 1; Livorno, 1900.

"Bollettino della Associazione 'Mathesis,'" Anno v., Num. 2; Livorno, 1900–1.

"Wiadomosci Matematyczne," Tom iv., Zeszyt 5, 6; Warsaw, 1900.

Tarleton, F. A.—"An Introduction to the Mathematical Theory of Attraction," 8vo; London, 1899.

Williamson B. and F. A. Tarleton.—"An Elementary Treatise on Dynamics," 8vo; London, 1900.

The following exchanges were received:—

"Proceedings of the Royal Society," Vol. lxvii., No. 438; 1900.

"Beiblätter zu den Annalen der Physik und Chemie," Bd. xxiv., St. 10; Leipzig, 1900.

"Bulletin de la Société Mathématique de France," Tome xxviii., Fasc. 4; Paris, 1900.

"Annales de la Faculté des Sciences de Toulouse," Série 2, Tome ii., Fasc. 1; Paris, 1900.

"Bulletin of the American Mathematical Society," Series 2, Vol. vii., No. 2; New York, 1900.

"Bulletin des Sciences Mathématiques," Série 2, Tome xxiv., Sep.; Paris, 1900.

"Annali di Matematica," Serie 3, Tomo v., Fasc. 1, Nov.; Milano, 1900.

"Atti della Reale Accademia dei Lincei—Rendiconti," Sem. 2, Vol. ix., Fasc. 8, 9, 10; Roma, 1900.

"Berichte über die Verhandlungen der Königl. Sächs. Gesellschaft der Wissenschaften zu Leipzig," Bd. lii., No. 5; 1900.

"Nyt Tidsskrift for Matematik," A. Aargang xi., Nr. 7, 8; Copenhagen, 1900

"Prace Matematyczno-Fizyczne," Tomo xi.; Warsaw, 1900.

"Proceedings of the Royal Irish Academy," Series 3, Vol. vi., No. 1, Oct.; Dublin, 1900.

Note on the Inflexions of Curves with Double Points. *By* H. W. Richmond.

Received November 27th, 1900. Read December 13th, 1900.

Apart from curves of the third order, our knowledge of the properties of the system of points of inflexion of a plane curve is very small. The inflexions of a non-singular curve U of order m form the complete family of intersections of U with a covariant curve, H the Hessian, of order $3m-6$. The nature of the intersection of U and H at an ordinary node or cusp is considered in the formation of Plücker's equations. At a point of higher singularity the nature of the intersection has been studied by Brill,[*] Kötter,[†] and others, and, more recently, in an extended form, by Segre.[‡] But these investigations must be ranked as algebra rather than geometry, and deal with the abnormal intersections of U and H which do not count among the points of inflexion of U, not with the simple intersections which are the points of inflexion—except in so far as they determine the number of the latter. As to the reality of the points of inflexion, Klein,[§]

---

[*] *Mathematische Annalen*, Band xiii., p. 175.

[†] *Ibid.*, Band xxxiv., p. 123.

[‡] *Rendiconti d. R. Accad. dei Lincei*, Series 5, Vol. iv. (2), 1895.

[§] *Mathematische Annalen*, Band x., p. 199.

extending a result concerning curves of the fourth order due to Zeuthen,[*] has proved that in a non-singular curve only one-third of the total number of inflexions can be real, and as many as one-third may be real; he has also given a relation which throws much light on the matter in the case of a curve endowed with nodes and cusps.

In curves of the fourth order our knowledge is fuller, and I have therefore made an attempt to bring together the known properties of the inflexions of quartic curves which have one or two or three double points. I have not considered how the theorems are modified when the double point is of a special kind, as a cusp or flecnode; on the other hand, I have added a few results which I have not seen previously stated, have summed up the whole into two propositions, and established that a partial extension to curves of higher order is valid. The question of reality as regards inflexions of a quartic has been answered very completely in a dissertation recently presented to the faculty of Bryn Mawr College, Pa., U.S.A., by Miss R. Gentry,[†] which contains a catalogue with figures of possible shapes of all quartic curves, and brings to a worthy conclusion the task begun by Zeuthen in the paper already mentioned. The inflexions of a quartic with 0, 1, 2, 3 ordinary double points number 24, 18, 12, 6 respectively.[‡]

(1) *Quartics with one node.*—The eighteen inflexions have been shown by Brill[§] to lie on a curve of the fifth order, which cuts the quartic in two further points collinear with the two points where the nodal tangents cut the curve. These two further points are points of the highest importance in the geometry of the curve; I have proved

---

[*] *Mathematische Annalen*, Band VII., p. 410.

[†] *On the Forms of Plane Quartic Curves*, published by Robert Drummond, New York.

[‡] The researches of Caporali should be mentioned, although they led to few definite results; see *Memorie di Geometria*, published in Naples, 1888 (also *Rendiconti dell' Accad. delle Sc. di Napoli*, Vol. XXI., 1882; and Segre, "Alcune idee di Ettore Caporali," *Ann. di Mat.*, Ser. 2, Vol. XX., 1892).

Gerbaldi (*Rendiconti del Circolo Matematico di Palermo*, Vol. VII., 1893, p. 178) has remarked a special case which he describes as "notevolissimo," when the inflexions fall into six sets of four, any two sets lying on a conic. A little reflection shows that Gerbaldi's quartic may be represented by an equation

$$ax^4+by^4+cz^4+2fy^2z^2+2gz^2x^2+2hx^2y^2 = 0.$$

His result is trivial, since, if (x, y, z) be an inflexion, so also are $(\pm x, \pm y, \pm z)$. Separate instances of curves of any order which possess symmetry of sundry kinds, symmetry which must be shared by the points of inflexion, might be multiplied *ad infinitum*.

[§] *Mathematische Annalen*, Band XIII., pp. 103 and 517. The second paper contains corrections of some unsound reasoning in the too simple proofs of the first paper.

elsewhere* that they are the intersections of the uninodal quartic with the conic that passes through the six contacts of the tangents from the node. Their importance arises chiefly from the fact that they form with the node the singular points of a quadric transformation by which the quartic is changed into itself. If they be projected to the circular points at infinity, the curve is inverse to itself in the sense of elementary geometry, the node being the centre of inversion.

(2) *Quartics with two nodes.*—The symbolic equations of the doubly infinite linear system of curves of the fourth order that pass through the twelve inflexions are obtained by Brill in the papers already cited. One such curve is the quartic itself, and a second passes through both nodes; and, generally, Brill shows that any quartic through the inflexions cuts out on the binodal quartic four further points that lie on a conic with the four points where the nodal tangents cut the curve. A simple method of investigating the inflexions is to express the coordinates of the points of the curve as elliptic functions of a parameter u. If α_1, α_2 be the values of u at one node, β_1, β_2 those at the other node, the parameters, $u_1, u_2, u_3, \ldots, u_{4n}$, of the $4n$ intersections of a curve of order n with the binodal quartic satisfy three conditions:

$$\Sigma u_r = n\,(\alpha_1+\alpha_2+\beta_1+\beta_2) \quad (r = 1, 2, 3, \ldots, 4n),$$

$$\Pi\,\frac{\sigma\,(\alpha_1-u_r)}{\sigma\,(\alpha_2-u_r)} = \left[\frac{\sigma\,(\alpha_1-\beta_1)\,\sigma\,(\alpha_1-\beta_2)}{\sigma\,(\alpha_2-\beta_1)\,\sigma\,(\alpha_2-\beta_2)}\right]^n,$$

$$\Pi\,\frac{\sigma\,(\beta_1-u_r)}{\sigma\,(\beta_2-u_r)} = \left[\frac{\sigma\,(\beta_1-\alpha_1)\,\sigma\,(\beta_1-\alpha_2)}{\sigma\,(\beta_2-\alpha_1)\,\sigma\,(\beta_2-\alpha_2)}\right]^n.$$

The parameters, $i_1, i_2, i_3, \ldots, i_{12}$, of the twelve inflexions are given by

$$\begin{vmatrix} \wp\,(u-\alpha_1)-\wp\,(u-\alpha_2), & \wp\,(u-\beta_1)-\wp\,(u-\beta_2) \\ \wp'(u-\alpha_1)-\wp'(u-\alpha_2), & \wp'(u-\beta_1)-\wp'(u-\beta_2) \end{vmatrix} = 0.$$

Therefore $$\Sigma\,(i_r) = 3\,(\alpha_1+\alpha_2+\beta_1+\beta_2) \quad (r = 1, 2, 3, \ldots, 12),$$

$$\Pi\,\frac{\sigma\,(\alpha_1-i_r)}{\sigma\,(\alpha_2-i_r)} = \frac{\sigma\,(\alpha_1-\beta_1)\,\sigma\,(\alpha_1-\beta_2)\,\sigma\,(2\alpha_1-\beta_1-\beta_2)}{\sigma\,(\alpha_2-\beta_1)\,\sigma\,(\alpha_2-\beta_2)\,\sigma\,(2\alpha_2-\beta_1-\beta_2)},$$

$$\Pi\,\frac{\sigma\,(\beta_1-i_r)}{\sigma\,(\beta_2-i_r)} = \frac{\sigma\,(\beta_1-\alpha_1)\,\sigma\,(\beta_1-\alpha_2)\,\sigma\,(2\beta_1-\alpha_1-\alpha_2)}{\sigma\,(\beta_2-\alpha_1)\,\sigma\,(\beta_2-\alpha_2)\,\sigma\,(2\beta_2-\alpha_1-\alpha_2)}.$$

---

* *Quart. Jour. of Math.*, Vol. xxvi., p. 5. Compare W. R. W. Roberts, "On Uninodal Quartics," *Proc. Lond. Math. Soc.*, Vol. xxv., p. 151.

Now the tangents at the nodes cut the quartic in four points where the parameter u is equal respectively to

$$\beta_1+\beta_2-\alpha_1, \quad \beta_1+\beta_2-\alpha_2, \quad \alpha_1+\alpha_2-\beta_1, \quad \alpha_1+\alpha_2-\beta_2.$$

We show without difficulty that (i.) the curves of order $n+3$ which pass through the twelve inflexions, (ii.) the curves of order $n+1$ that pass through the four points where the nodal tangents intersect the curve, cut out on the binodal quartic the same sets of $4n$ points.*

(3) *Quartics with three nodes.*—The six inflexions and the six points in which the nodal tangents cut the curve are proved by Brill† to lie on two conics, which intersect the curve in the same two further points. To prove these theorems, we may express the coordinates of points on the curve as rational quartic functions of a parameter λ, in which form, if (α_1, α_2), (β_1, β_2), (γ_1, γ_2) be the pairs of values of λ at the three nodes, the three relations that connect the $4n$ parameters $(\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_{4n})$ of the quartic and a curve of order n are the three relations similar to

$$\Pi\,\frac{\alpha_1-\lambda_r}{\alpha_2-\lambda_r} = \left[\frac{(\alpha_1-\beta_1)(\alpha_1-\beta_2)(\alpha_1-\gamma_1)(\alpha_1-\gamma_2)}{(\alpha_2-\beta_1)(\alpha_2-\beta_2)(\alpha_2-\gamma_1)(\alpha_2-\gamma_2)}\right]^n \quad (r = 1, 2, 3, \ldots, 4n).$$

It is easy to see that the product

$$\Pi\left(\frac{\alpha_1-\lambda}{\alpha_2-\lambda}\right)$$

has the same value when λ receives six values that correspond (i.) to the inflexions, (ii.) to the intersections of the nodal tangents with the curve, (iii.) to the contacts of the tangents from the nodes. Hence, assuming Brill's theorem that the six inflexions lie on a conic, we see that the six intersections of the nodal tangents with the curve and

---

* In order that the twelve inflexions may lie on a cubic, I notice (*Quart. Jour. of Math.*, Vol. XXXII., p. 63) that only *a single condition*,

$$\wp(\alpha_1-\beta_1)+\wp(\alpha_2-\beta_2) = \wp(\alpha_1-\beta_2)+\wp(\alpha_2-\beta_1),$$

has to be satisfied—not, as might be expected, *three* conditions. The one condition being fulfilled, the nodal tangents cut the curve in four collinear points.

† *Mathematische Annalen*, Band XII., p. 90; Band XIII., p. 175. Compare Franz Meyer, *Apolarität und rationale Curven*, pp. 283–287, where a notable property of the two further points is obtained. If the equation of the trinodal quartic be, as in Salmon, *Higher Plane Curves*, p. 254,

$$ay^2z^2+bz^2x^2+cx^2y^2+2fx^2yz+2gy^2zx+2hz^2xy = 0,$$

the two further points are the two points where

$$afyz+bgzx+chxy = 0.$$

the six contacts of tangents from the nodes also lie on conics, the three conics all intersecting the quartic in the same two further points.

Having set down side by side these theorems on the inflexions of quartics,* we observe that they may be summed up in two propositions. The first is Brill's theorem that the inflexions of a trinodal quartic lie on a conic; the second is:—

On a curve of the fourth order which has none but ordinary double points, whether one, two, or three in number, the three point-groups formed, (i.) *of the* (18, 12, *or* 6) *points of an inflexion,* (ii.) *of the* (2, 4, *or* 6) *intersections of the nodal tangents with the curve, are coresidual.* Incidentally, it has been noticed that in the cases of the uninodal and trinodal curves the six points of contact of the tangents from the nodes are also coresidual with these two point-groups.†

I proceed to establish an extension of this result, viz.:—

On a curve of any order which has none but ordinary double points the inflexions and the points where the nodal tangents cut the curve constitute a pair of coresidual point-groups.

The double points must not be cusps or flecnodes, but must be formed by the crossing of two (real or imaginary) branches, the tangents at the point of crossing being distinct and having only normal (two-point) contact with the branch. Also the case when one of the nodal tangents goes through a second node must be barred out, or, at least, investigated separately.

Let U be a curve of order m with d ordinary double points, $O_1, O_2, O_3, \ldots$; let H be its Hessian of order $3m-6$. The two tangents at any one of the double points are distinct, and each cuts U in $m-3$ points other than the double point. Through the $2m-6$ points on the tangents at O_r draw a curve V_r of order $m-3$, not passing through any node or inflexion of U nor any intersection of U with another nodal tangent, and denote by G_r the point-group composed of its $(m-2)(m-3)$ other intersections with U.

---

* The inflexional tangents possess the following properties:—In the non-singular quartic they form the complete system of common tangents of two curves of class four and six respectively enveloped by lines on which the quartic cuts out an equianharmonic or a harmonic range. The twenty lines made up of the eighteen inflexional tangents and the two nodal tangents of a uninodal quartic are the complete system of common tangents of two curves of class four and five respectively. The twelve inflexional tangents of a binodal quartic and the four nodal tangents touch a singly infinite linear system of curves of class four. In a trinodal quartic. the six inflexional tangents, the six nodal tangents, and the six tangents from the nodes all touch conics; and the three conics touch one another at the same two points. It does not appear that these properties can be extended in any obvious way to curves of higher order.

† I am indebted to the referee for notice of the curious fact, concerning which I had fallen into error, that the points where the curve is touched by tangents from the nodes and the points where the curve is cut by tangents at the nodes do not form coresidual point-groups in the binodal quartic, although they do so in the uninodal and trinodal curve.

The intersections of U and H are made up of simple intersections at each inflexion of U and six-fold intersections of a particular kind at each double point, O_1, O_2, O_3, ... We proceed to construct a series of curves K_1, K_2, K_3, ..., of orders which increase in an arithmetical progression with common difference $m-5$, whereof K_1 has the same intersections with U as H, except that K_1 does not pass through O_1, but has a simple intersection with U at each point of the point-group G_1; K_2 has the same intersections with U as K_1, save that K_2 does not go through O_2, but has a simple intersection with U at each point of the point-group G_2, ...; K_r has the same intersections with U as K_{r-1}, save that K_r does not pass through O_r, but has a simple intersection with U at each point of the point-group G_r, ... Finally, we shall arrive at a curve of order

$$3m-6+d(m-5),$$

which has a simple intersection with U at each inflexion and at each point of all the point-groups G_1, G_2, G_3, ... Therefore the inflexions will have been proved residual to the aggregate of all the point-groups G_1, G_2, G_3, ...; and, by the construction of the last paragraph, the point-groups G_1, G_2, G_3, ... are residual to the points of intersection of the nodal tangents with the curve. Hence the inflexions and the intersections of the nodal tangents with the curve will have been proved to form two coresidual point-groups; that is to say, if any curve whatever pass through all the inflexions of U and cut U in a further group of points G, a second curve can be constructed which cuts U in the points G and the points where the nodal tangents cut U, and in no other point. It remains to investigate the method by which K_{r-1} is replaced by K_r.

Let $x=0$, $y=0$ be the tangents (whether real or imaginary) at O_r; $z=0$ a line that does not pass through O_r. With x, y, z as coordinates the equation of U is

$$xyz^{m-2}+(ax^3+by^3+cx^2y+dxy^2)\,z^{m-3}+(\dots)\,z^{m-4}+\&c.=0.$$

The coefficients a and b are debarred from vanishing by the condition that the branches through O_r are not inflected at O_r; thus the points where the tangents $x=0$, $y=0$ cut the curve U are determined by equations

$$x = 0, \quad by^3(z^{m-3}+p_1z^{m-4}y+p_2z^{m-5}y^2+\dots p_{m-3}y^{m-3}) = 0,$$
$$y = 0, \quad ax^3(z^{m-3}+q_1z^{m-4}x+q_2z^{m-5}x^2+\dots q_{m-3}x^{m-3}) = 0,$$

respectively; and the curve V_r, which is drawn through the $2m-6$ points of U other than O_r that lie on $x = 0$ and $y = 0$, has an equation of the form

$$V_r \equiv z^{m-3}+(p_1y+q_1x)\,z^{m-4}+(p_2y^2+q_2x^2)\,z^{m-5}+\dots$$
$$\dots+(p_{m-3}y^{m-3}+q_{m-3}x^{m-3})+xyF_{m-5} = 0,$$

F_{m-5} being a function of x, y, z of degree $m-5$. We may therefore write the equation of U in the form

$$U \equiv xyF_{m-2}+(ax^3+by^3)\,V_r = 0,$$

F_{m-2} denoting a function of x, y, z of order $m-2$, the terms z^{m-2} and z_{m-3} being present in F_{m-2} and V_r respectively with coefficients unity, and a and b being different from zero.

We suppose that a curve K_{r-1} of degree l, where

$$l = 3m-6+(r-1)(m-5),$$

has been constructed, which has simple intersections with U at each of the inflexions of U, and at each point of each of the point-groups G_1, G_2, ..., G_{r-1}, and has a six-fold intersection of a special type at each of the $d-r+1$ double points O_r, O_{r+1}, O_{r+2}, ... ; K_{r-1} can have no further intersection with U.

Now assume for the moment that K_{r-1} is represented by an equation of the form

$$K_{r-1} \equiv xy\Phi_{l-2}+(ax^3+by^3)\,\Phi_{l-3} = 0,$$

where Φ_{l-2}, Φ_{l-3} are functions of x, y, z of orders $l-2$ and $l-3$ respectively, headed by the terms λz^{l-2} and μz^{l-3} respectively. The coefficients λ and μ possibly vanish, but it will appear that they cannot be equal and so cannot vanish simultaneously.* If, then, we have

$$xyK_r \equiv U\Phi_{l-3}-K_{r-1}V_r,$$

or

$$K_r \equiv F_{m-2}\Phi_{l-3}-\Phi_{l-2}V_r,$$

the curve $K_r = 0$ of order $l+m-5$ passes through all the simple intersections of U and K_{r-1}, all the points of the point-group G_r (which contains all the intersections of U and V_r which do not lie on $x = 0$

---

* If λ vanishes, K_{r-1} has a triple point at O_r, but the number of intersections of K_{r-1} and U that coalesce at O_r is not affected.

or $y = 0$, and therefore lie on $F_{m-2} = 0$), and has a six-fold intersection with U at each of the double points $O_{r+1}, O_{r+2}, \dots$. Thus K_r cannot cut U in any further points, and in particular cannot go through O_r, as it would do if λ and μ were equal; the possibility of λ and μ being equal has, in fact, been excluded, in some way which we need not stop to consider, by our assumptions concerning the curves $V_1, V_2, \dots, V_{r-1}$.

We *assume* again that in replacing K_{r-1} by K_r in the manner just explained we have done nothing that prevents us from afterwards applying the same treatment to any one of the other double points in which U and K_{r-1} intersect. The two assumptions are not in reality different; we shall justify both if we prove that H and all the curves $K_1, K_2, K_3, \dots, K_{r-1}$ introduced up to the stage at which any particular double point O_r is singled out for treatment fall under the form

$$xy\Phi_{l-2}+(ax^3+by^3)\,\Phi_{l-3}=0,$$

already assumed for K_{r-1}, the quantity l here denoting the order of the curve under consideration at the moment, and Φ_{l-2}, Φ_{l-3} standing for functions of x, y, z of order $l-2$ and $l-3$ respectively, headed by terms λz^{l-2} and μz^{l-3}.

Now H is well known and easily proved to be of this form, the values of λ and μ being $(m-2)(m-1)$ and $-m(m-1)$ respectively. To derive K_1 we take the difference of H multiplied by V_1 and U multiplied by some other function, and can reject a quadratic factor which represents the pair of factors at the node O_1; this quadratic factor cannot vanish when $x = 0$ and $y = 0$ on account of the conditions originally imposed. Hence K_1 is of the form assumed, the possibility of λ and μ being zero being taken into account; since the order in which the several double points are treated is arbitrary, we might consider O_r next; thus the previous proof that λ and μ are unequal is valid, and λ and μ are not both zero. The process may now be applied to $O_2, O_3, \dots$, till the time for dealing with O_r arrives.

Q.E.D.

The inflexions of elliptic curves ($p = 1$) possess certain special properties. On such a curve, being of order m, there are in the general case $\frac{1}{2}m(m-3)$ double points and $3m$ inflexions; the double points lie on a curve of order $m-3$, and constitute the complete system of its intersections with the elliptic curve. When the coordinates of the points of the elliptic curve are expressed as elliptic functions of a parameter u of the form

$$k+\left(k_0+k_1\frac{d}{du}+k_2\frac{d^2}{du^2}+\dots+k_{n-2}\frac{d^{n-2}}{du^{n-2}}\right)\wp u,$$

the $3m$ parameters of the inflexions are the zeroes of the determinant whose constituents are the three coordinates and their first and second differential coefficients with respect to u; the sum of the parameters of the $3m$ inflexions therefore vanishes, and a curve of order m other than the given elliptic curve will pass through all the double points and the $3m$ inflexions. Thus, when $p = 1$, it is possible to replace the Hessian by a curve of order m which, like the Hessian, has a simple intersection with the given curve at each inflexion; but, whereas the Hessian has a double point at each double point of the given curve, counting as a six-fold intersection, the new curve only passes through the double point

---

The Syzygetic Theory of Orthogonal Binariants. *By* E. B. ELLIOTT. Read and received December 13th, 1900.

1. Attention has been redirected to systems of orthogonal invariants and covariants of binary forms by Major MacMahon in a paper read at the 1900 meeting of the British Association. His method is symbolical. The following pages are, it is believed, quite independent of his work. Their aim is to show that a complete syzygetic theory of the concomitants in question can be based on very elementary and simple considerations.

In a binary p-ic, in fact, the complete irreducible system of non-absolute orthogonal concomitants consists of a pair $x \pm \iota y$ of linear universal covariants and $p+1$ linear invariants; and for a system of a p_1-ic, a p_2-ic, &c., it consists of $x \pm \iota y$ and p_1+1, p_2+1, &c., linear invariants of the p_1-ic, the p_2-ic, &c., separately. The theory of the complete irreducible system of *absolute* orthogonal concomitants for a given p-ic or system is, in effect, the theory of irreducible products, obeying a certain law of isobarism, of the appropriate linear system.

In the relation expressive of the invariancy for all linear transformations of a concomitant of a quantic or quantics, the factor is well known to be always a power of the modulus. All proofs of this depend for their validity on the irreducibility of the general modulus. No such fact holds as to concomitants which have the property of invariancy only for a restricted class of linear transformations, in case the modulus for that class be resoluble into factors. For instance, in expressions of invariancy for the class of transformations

$$x = lX - mY, \quad y = mX + lY,$$

the factor may be a product of different powers of $l + \iota m$ and $l - \iota m$. In particular, for the direct orthogonal transformation

$$x = X\cos\theta - Y\sin\theta, \quad y = X\sin\theta + Y\cos\theta,$$

the factor in an expression of invariancy will be a positive zero or negative power of $e^{\iota\theta}$.

Orthogonal invariants, &c., which are non-absolute for direct turning are left out of sight in chap. xv. of my *Algebra of Quantics.* They are not left out of sight in Andoyer's *Théorie des Formes;* but M. Andoyer's direction to find them (p. 143) by first investigating all absolute concomitants, and then combining $x + \iota y$ with the system found, reverses the order which will be seen to be the one readily applicable to the construction of syzygetic theory.

2. From $x = X\cos\theta - Y\sin\theta, \quad y = X\sin\theta + Y\cos\theta,$ (1)

it at once follows that

$$\left.\begin{aligned} X + \iota Y &= e^{-\iota\theta}(x + \iota y) \\ X - \iota Y &= e^{\iota\theta}(x - \iota y) \end{aligned}\right\}. \tag{2}$$

Thus $x + \iota y$ and $x - \iota y$, which call ξ and η, are fundamental—universal—concomitants, of factors $e^{-\iota\theta}$, $e^{\iota\theta}$ respectively. $\xi^m\eta^n$ is one of factor $e^{-\iota(m-n)\theta}$. Any rational integral function of x and y, with numerical coefficients, may be given the form

$$\Sigma\lambda_{mn}\xi^m\eta^n,$$

by putting $\frac{1}{2}(\xi + \eta)$ and $\frac{1}{2\iota}(\xi - \eta)$ for x and y. It will be a universal concomitant if and only if for each term, when it is thus written, $m - n$ is the same.

Moreover, $\frac{\partial}{\partial x} + \iota\frac{\partial}{\partial y}$ and $\frac{\partial}{\partial x} - \iota\frac{\partial}{\partial y}$ are fundamental invariant operators, of factors $e^{-\iota\theta}$, $e^{\iota\theta}$ respectively. If, in fact,

$$F(X, Y) \equiv f(x, y)$$

be any equivalence, we have

$$\left(\frac{\partial}{\partial X} + \iota\frac{\partial}{\partial Y}\right)^r \left(\frac{\partial}{\partial X} - \iota\frac{\partial}{\partial Y}\right)^s F(X, Y)$$
$$\equiv e^{-\iota(r-s)\theta}\left(\frac{\partial}{\partial x} + \iota\frac{\partial}{\partial y}\right)^r \left(\frac{\partial}{\partial x} - \iota\frac{\partial}{\partial y}\right)^s f(x, y). \tag{3}$$

For shortness, write F_{rs} and $e^{-\iota(r-s)\theta}f_{rs}$ for the two sides here. A consequence is that

$$F_{r_1s_1}F_{r_2s_2}F_{r_3s_3}\dots = e^{-\iota(\Sigma r-\Sigma s)\theta}f_{r_1s_1}f_{r_2s_2}f_{r_3s_3}\dots. \qquad (4)$$

This affords us the means of writing down all rational integral differential equations which are unaltered in form by any transformation such as (1) applied to the independent variables, and of deciding whether a given equation has the property. Replace, in an equation

$$\Sigma A x^{\alpha}y^{\beta}z^{\gamma}\frac{\partial^{m_1+n_1}z}{\partial x^{m_1}\partial y^{n_1}}\frac{\partial^{m_2+n_2}z}{\partial x^{m_2}\partial y^{n_2}}\dots = 0,$$

x, y by $\frac{1}{2}\{(x+\iota y)+(x-\iota y)\}$, $\frac{1}{2\iota}\{(x+\iota y)-(x-\iota y)\}$ respectively, and $\frac{\partial}{\partial x}$, $\frac{\partial}{\partial y}$ by the like linear functions of $\frac{\partial}{\partial x}+\iota\frac{\partial}{\partial y}$, $\frac{\partial}{\partial x}-\iota\frac{\partial}{\partial y}$, thus giving it the form

$$\Sigma B(x+\iota y)^{\alpha'}(x-\iota y)^{\beta'}z^{\gamma'}\left(\frac{\partial}{\partial x}+\iota\frac{\partial}{\partial y}\right)^{r_1}\left(\frac{\partial}{\partial x}-\iota\frac{\partial}{\partial y}\right)^{s_1}z$$
$$\times\left(\frac{\partial}{\partial x}+\iota\frac{\partial}{\partial y}\right)^{r_2}\left(\frac{\partial}{\partial x}-\iota\frac{\partial}{\partial y}\right)^{s_2}z\dots = 0,$$

from which the transformation (1) produces the like form in X, Y with each B replaced by the corresponding $Be^{\iota(\alpha'-\beta'+\Sigma r-\Sigma s)\theta}$. The necessary and sufficient condition for permanence of form is then that for all terms

$$\alpha'-\beta'+\Sigma r-\Sigma s = \text{const.}$$

The property common to equations with this permanence is that their general solutions are unaltered in functional form when in them $x+\iota y$ is multiplied, and $x-\iota y$ divided, by any the same constant $e^{\iota\theta}$.

3. Take now the infinitesimal transformation

$$x = X - Y\theta', \quad y = X\theta' + Y \qquad (4)$$

included in (1). To express properties of invariancy for the one-parameter group (1) it, we know, suffices to express the facts for (4). For a form K associated with

$$u \equiv (a_0, a_1, a_2, \dots, a_p)(x, y)^p \qquad (5)$$

to have the property of invariancy for (1) it is necessary and suffices that its infinitesimal increment, when X, Y from (4) are substituted in it for x, y, and the consequential substitutions for $a_0, a_1, a_2, \dots, a_p$ are made, be a multiple of $\theta' K$. Accordingly the condition is that, for some value of λ,

$$\left(\Omega - O - y\frac{\partial}{\partial x} + x\frac{\partial}{\partial y}\right) K = \lambda K, \tag{6}$$

where

$$\Omega \equiv a_0\frac{\partial}{\partial a_1} + 2a_1\frac{\partial}{\partial a_2} + \dots + pa_{p-1}\frac{\partial}{\partial a_p}, \tag{7}$$

$$O \equiv pa_1\frac{\partial}{\partial a_0} + (p-1)\,a_2\frac{\partial}{\partial a_1} + \dots + a_p\frac{\partial}{\partial a_{p-1}}. \tag{8}$$

We have already found the two solutions $x \pm \iota y$, of equations such as (6), which are linear in the variables and free from the coefficients. Let us now consider solutions linear in the coefficients in (5) and free from the variables, *i.e.*, linear orthogonal *invariants* of u.

For

$$k_0 a_0 + k_1 a_1 + k_2 a_2 + \dots + k_p a_p \tag{9}$$

to be such an invariant the equations to be satisfied by λ and the k's are

$$\left.\begin{array}{ll} k_1 & = \lambda k_0 \\ 2k_2 - pk_0 & = \lambda k_1 \\ 3k_3 - (p-1)\,k_1 & = \lambda k_2 \\ \dots \quad \dots & \dots \\ pk_p - 2k_{p-2} & = \lambda k_{p-1} \\ -k_{p-1} & = \lambda k_p \end{array}\right\}, \tag{10}$$

and there is consequently one set of values of ratios of the k's corresponding to every value of λ which satisfies the equation

$$\left|\begin{array}{cccccccc} \lambda & -1 & & & & & & \\ p & \lambda & -2 & & & & & \\ & p-1 & \lambda & -3 & & & & \\ & & & \cdots\cdots & & & & \\ & & & & \cdots\cdots & & & \\ & & & & 3 & \lambda & -(p-1) & \\ & & & & & 2 & \lambda & -p \\ & & & & & & 1 & \lambda \end{array}\right| = 0. \tag{11}$$

The direct algebraical solution of this equation presents difficulties. But it will be seen indirectly that the equation must, in fact, be

$$(\lambda^2+1^2)(\lambda^2+3^2)\dots(\lambda^2+p^2) = 0$$

or

$$\lambda\,(\lambda^2+2^2)(\lambda^2+4^2)\dots(\lambda^2+p^2) = 0,$$

according as p is odd or even. In fact,

$$\Omega - O - y\frac{\partial}{\partial x} + x\frac{\partial}{\partial y}$$

annihilates $$u \equiv (a_0, a_1, a_2, \ldots, a_p)(x, y)^p, \tag{5}$$

to which apply the transformation $x = \frac{1}{2}(\xi+\eta)$, $y = \frac{1}{2\iota}(\xi-\eta)$ of § 2, and write it

$$u \equiv (a_0', a_1', a_2', \ldots, a_p')(\xi, \eta)^p. \tag{11}$$

Now, from the term $\binom{p}{r} a_r' \xi^{p-r}\eta^r$ in this, $-y\frac{\partial}{\partial x} + x\frac{\partial}{\partial y}$ produces

$$\iota\,(p-2r)\binom{p}{r} a_r' \xi^{p-r}\eta^r.$$

Consequently $\Omega - O$ must produce from it

$$-\iota\,(p-2r)\binom{p}{r} a_r' \xi^{p-r}\eta^r.$$

In other words, $$(\Omega - O)\,a_r' = -\iota\,(p-2r)\,a_r' \quad (r = 0, 1, 2, \ldots, p). \tag{12}$$

There are then $p+1$ distinct values of λ which make the equations (10) consistent, namely, the values $-\iota p$, $-\iota(p-2)$, ..., $\iota(p-2)$, ιp; and $p+1$ distinct corresponding linear orthogonal invariants (9), namely, the coefficients a_0', a_1', a_2', ..., a_p' in (11).

These $p+1$ linear orthogonal invariants are linearly independent. For, were the coefficients in (11) linearly connected, so would be the $p+1$ linear functions of them a_0, a_1, a_2, ..., a_p; but these are general.

4. To find the expressions for these linear invariants, we notice from (11) that

$$\frac{\partial^p}{\partial\xi^{p-r}\partial\eta^r}\,u = p!\,a_r',$$

and we also observe that

$$\frac{\partial}{\partial\xi} = \tfrac{1}{2}\left(\frac{\partial}{\partial x} - \iota\frac{\partial}{\partial y}\right), \quad \frac{\partial}{\partial\eta} = \tfrac{1}{2}\left(\frac{\partial}{\partial x} + \iota\frac{\partial}{\partial y}\right). \tag{13}$$

Thus $$a_r' = \frac{1}{p!\,2^p}\left(\frac{\partial}{\partial x} - \iota\frac{\partial}{\partial y}\right)^{p-r}\left(\frac{\partial}{\partial x} + \iota\frac{\partial}{\partial y}\right)^r u$$

$$(r = 0, 1, 2, \ldots, p). \tag{14}$$

Let us now change the notation, and write I_{p-2r} for $2^p a_r'$, thus taking for our $p+1$ independent linear invariants

$$I_p,\ I_{-p},\ I_{p-2},\ I_{-p+2},\ \ldots,\ I_1,\ I_{-1}$$

if p is odd, and $$I_p,\ I_{-p},\ I_{p-2},\ I_{-p+2},\ \ldots,\ I_2,\ I_{-2},\ I_0$$

if p is even, where, for every s from 0 to the greatest integer in $\frac{1}{2}p$,

$$I_{\pm(p-2s)} = \frac{1}{p!}\left(\frac{\partial}{\partial x} \mp \iota \frac{\partial}{\partial y}\right)^{p-s} \left(\frac{\partial}{\partial x} \pm \iota \frac{\partial}{\partial y}\right)^{s} u$$

$$= \frac{1}{p!}\left(\frac{\partial}{\partial x} \mp \iota \frac{\partial}{\partial y}\right)^{p-2s} \left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\right)^{s} u. \tag{15}$$

Now, to adopt a notation* in which all the "symbolic" theory of forms can be advantageously expressed without the use of any symbol which has not actual meaning either as a quantity or as a differential operator,

$$u \equiv (a_0, a_1, a_2, \dots, a_p)(x, y)^p$$

$$\equiv (x+yd)^p a_0, \tag{16}$$

where $$d \equiv a_1 \frac{\partial}{\partial a_0} + a_2 \frac{\partial}{\partial a_1} + \dots + a_p \frac{\partial}{\partial a_{p-1}}. \tag{17}$$

Hence (15) gives

$$I_{\pm(p-2s)} = \frac{1}{(p-2s)!}\left(\frac{\partial}{\partial x} \mp \iota \frac{\partial}{\partial y}\right)^{p-2s} (x+yd)^{p-2s} (1+d^2)^s a_0$$

$$= (1 \mp \iota d)^{p-2s} (1+d^2)^s a_0$$

$$= (1 \mp \iota d)^{p-2s} (a_0, a_2, a_4, \dots, a_{2s})(1, 1)^s$$

$$= \{(a_0, a_2, \dots, a_{2s})(1, 1)^s, (a_1, a_3, \dots, a_{2s+1})(1, 1)^s, \dots$$

$$\dots, (a_{p-2s}, a_{p-2s+1}, \dots, a_p)(1, 1)^s\} (1, \mp \iota)^{p-2s}, \tag{18}$$

a pair of expressions of conjugate imaginary form. When p is even the single I_0 given by $s = \frac{1}{2}p$ is of real form, namely,

$$(a_0, a_2, a_4, \dots, a_p)(1, 1)^{\frac{1}{2}p}. \tag{19}$$

The factor in the expression of invariancy of any of these linear invariants I_m is the power of $e^{\iota\theta}$ whose index is the suffix m. For, in (15), $\frac{\partial}{\partial x} \mp \iota \frac{\partial}{\partial y}$ are by § 2 invariant operators of respective factors $e^{\pm\iota\theta}$. The doctrine of the infinitesimal substitution of § 3 gives the same information.

---

* Called attention to by Mr. Kempe, *Proc. Lond. Math. Soc.*, Vol. xxiv., p. 102.

[The kindness of Major MacMahon supplies me with a note on the convenience of the pure German symbolism, which he has adopted and extended in his own work on orthogonal systems.

Let the quantic be $(a_1 x_1 + a_2 x_2)^p \equiv \alpha_x^p$, where a_1, a_2 are umbræ. Invariant umbral expressions are $a_1 - \iota a_2 \equiv \alpha_1$ and $a_1 + \iota a_2 \equiv \alpha_2$; and $x_1 + \iota x_2 \equiv \xi_1$, $x_1 - \iota x_2 \equiv \xi_2$ are invariant. Now $2a_x \equiv \alpha_1 \xi_1 + \alpha_2 \xi_2 \equiv \alpha_\xi$. Also all products of integral powers of α_1 and α_2 are invariants in symbolic form for some value of p, so that in $\frac{1}{2^p}\alpha_\xi^p$ all the coefficients are linear invariants, and the variables are covariants. The form $\frac{1}{2^p}\alpha_\xi^p$, *i.e.* (22A), is canonical.

In place of my I notation he would recommend one of double suffixes. Thus, in the case of the p-ic α_ξ^p, he would regard $I_{p\,0}, I_{p-1\,1}, I_{p-2\,2}, \dots, I_{0\,p}$ as the most expressive notation for $\alpha_1^p, \alpha_1^{p-1}\alpha_2, \alpha_1^{p-2}\alpha_2^2, \dots, \alpha_2^p$, or for the linear invariants (14).]

Every product $I_m I_{-m}$ of a conjugate pair is a quadratic absolute orthogonal invariant of real form.

Examples.—For low values of p the linear systems are as follows:—

(i.) For the linear form $ax+by$,

$$I_1,\ I_{-1} \equiv a \mp \iota b;\ \text{factors } e^{\pm\iota\theta}.$$

(ii.) For the quadratic $ax^2+2bxy+cy^2$,

$$I_2,\ I_{-2} \equiv a \mp 2\iota b - c;\ \text{factors } e^{\pm 2\iota\theta},$$
$$I_0 \equiv a+c;\ \text{factor } 1.$$

(iii.) For the cubic $(a, b, c, d)(x, y)^3$,

$$I_3,\ I_{-3} \equiv a \mp 3\iota b - 3c \pm \iota d;\ \text{factors } e^{\pm 3\iota\theta},$$
$$I_1,\ I_{-1} \equiv a+c \mp \iota(b+d);\ \text{factors } e^{\pm\iota\theta}.$$

(iv.) For the quartic $(a, b, c, d, e)(x, y)^4$,

$$I_4,\ I_{-4} \equiv a \mp 4\iota b - 6c \pm 4\iota d + e;\ \text{factors } e^{\pm 4\iota\theta},$$
$$I_2,\ I_{-2} \equiv a+c \mp 2\iota(b+d) - (c+e);\ \text{factors } e^{\pm 2\iota\theta},$$
$$I_0 \equiv a+2c+e;\ \text{factor } 1.$$

(v.) For the quintic $(a, b, c, d, e, f)(x, y)^5$,

$$I_5,\ I_{-5} \equiv a \mp 5\iota b - 10c \pm 10\iota d + 5e \mp \iota f;\ \text{factors } e^{\pm 5\iota\theta},$$
$$I_3,\ I_{-3} \equiv a+c \mp 3\iota(b+d) - 3(c+e) \pm \iota(d+f);\ \text{factors } e^{\pm 3\iota\theta},$$
$$I_1,\ I_{-1} = a+2c+e \mp \iota(b+2d+f);\ \text{factors } e^{\pm\iota\theta}.$$

5. It must be remarked that these systems of linear orthogonal invariants are obtained as invariant only for *direct* orthogonal transformations

$$x = X\cos\theta - Y\sin\theta,\quad y = X\sin\theta + Y\cos\theta. \tag{1}$$

A *skew* orthogonal transformation

$$x = X\cos\theta + Y\sin\theta,\quad y = X\sin\theta - Y\cos\theta, \tag{20}$$

i.e., the result of the sequence of a direct orthogonal transformation and a change of sign of Y and second, fourth, &c., coefficients in the transformed p-ic, produces as equal to $e^{\iota m\theta}I_m$, not the function I_m of final coefficients, but the conjugate I_{-m}. The real quadratic product $I_m I_{-m}$ is absolutely invariant for skew as well as direct transformations.

In like manner $\xi \equiv x+\iota y$ of factor $e^{-\iota\theta}$ and $\eta \equiv x-\iota y$ of factor $e^{\iota\theta}$ are invariant only for direct orthogonal transformations. For skew transformations they are interchanged as well as affected by factors. The product $\xi\eta \equiv x^2+y^2$, the absolute, is, of course, absolutely invariant for skew as well as direct transformations.

A product $I_m^\mu I_n^\nu I_q^\kappa \ldots \xi^\alpha \eta^\beta$ involves y and the alternate coefficients a_1, a_3, a_5, ... only to even dimensions in its real part and only to odd dimensions in its part affected by ι. It is an orthogonal invariant or covariant for direct transformations, which is absolute if, and only if,

$$m\mu+n\nu+q\kappa+\ \ldots\ -\alpha+\beta=0\,; \tag{21}$$

and, if this be the case, its conjugate $I_{-m}^\mu I_{-n}^\nu I_{-q}^\kappa \ldots \eta^\alpha \xi^\beta$ will also be absolute. For skew transformations neither product will be absolute, or indeed invariant, unless the products are identical, *i.e.*, unless their form be the real one $(I_m I_{-m})^\mu (I_n I_{-n})^\nu \ldots (\xi\eta)^\alpha$. Half the sum of the two, however, and $\dfrac{1}{2\iota}$ times their difference, will, if (21) be satisfied, be real and invariant also for skew transformations. The former will be absolute and the latter will have the factor -1 for the skew case, though absolute for the direct.

The systems presently investigated as systems of absolute orthogonal invariants will be absolute for direct transformations. To avoid repetition it may be stated, once for all, that when for any quantic or quantics a system of products of the I's and ξ, η, say the products A, B, ... P, P', Q, Q' ..., in which the pairs P, P', &c., are conjugate has been seen to form a complete irreducible system of absolute orthogonal invariants, or invariants and covariants, for direct transformations, the completed facts will be that a direct absolute invariant or covariant when expressed, as it can be, rationally and integrally in terms of

$$A,\ B, \ldots,\quad \tfrac{1}{2}(P+P'),\quad \frac{1}{2\iota}(P-P'),\quad \tfrac{1}{2}(Q+Q'),\quad \frac{1}{2\iota}(Q-Q'), \ldots,$$

will be also invariant for skew transformations if, and only if, in every one of the products of which it consists the number of difference factors $P-P'$, $Q-Q'$, ... is either odd or even. Only in the case of evenness is the invariancy for skew transformations absolute. In the case of oddness the factor is -1.

6. The system of $p+1$ independent linear orthogonal invariants

$$\left.\begin{array}{ll} & I_p,\ I_{p-2},\ \ldots,\ I_{-p+2},\ I_{-p} \\ \text{or} & a'_0,\ a'_1,\ \ldots,\ a'_{p-1},\ a'_p \end{array}\right\} \qquad (22)$$

constitutes the complete irreducible system of non-absolute and absolute direct orthogonal invariants for one p-ic. In fact, remembering how (11) was formed from (5), we recognize that every rational integral function of $a_0, a_1, a_2, \ldots, a_p$ can be rationally and integrally expressed in terms of $a'_0, a'_1, a'_2, \ldots, a'_p$. In particular, then, any invariant can. The one requirement and sufficiency that a rational integral function thus expressed may possess invariancy is that the sum of the suffixes—in either the a' or the I notation—be constant throughout, because I_m is of factor $e^{m\iota\theta}$.

The same system (22) with the addition of ξ and η is the complete irreducible system of direct orthogonal invariants and covariants, in like manner. The sum of the suffixes of the I's, diminished by the exponent of ξ and increased by that of η, is what has to be constant throughout a rational integral function of the system which is a covariant.

Notice that the p-ic is not one of its own irreducible system. Its expression by means of that system is

$$\frac{1}{2^p}\,(I_p,\ I_{p-2},\ \ldots,\ I_{-p+2},\ I_{-p})(\xi,\ \eta)^p. \qquad (22\text{A})$$

Products, of one degree, of members of the system (22) cannot be connected by any syzygy. Indeed, no relation connects $a'_0, a'_1, \ldots, a'_p$, which are quite independent, because the equally numerous linear functions $a_0, a_1, \ldots, a_p$ of them are. Neither can products of one degree and order of (22) and ξ, η be connected, for a like reason.

This syzygetic independence of products, and the constancy of sums of suffixes in the terms of such invariants as are sums of products, give us means of applying partition theory to estimate the number of linearly independent orthogonal invariants which have the same factor.

Write ρ for $e^{\iota\theta}$. The factor which occurs in the expression of invariancy of a product of powers of $I_p, I_{p-2}, \ldots, I_{-p+2}, I_{-p}$ for which the sum of suffixes is κ, or of a linear function of such products with the same κ, is then ρ^κ. If we adopt the notation $a'_0, a'_1, \ldots, a'_p$, the sum of suffixes, w say, is Σr, where $\kappa = \Sigma\,(p-2r)$, so that, if i be the degree of the product, or of each product,

$$\kappa = ip - 2w,$$

i.e.,

$$w = \tfrac{1}{2}\,(ip - \kappa).$$

There is, then, a one to one correspondence between orthogonal invariants of degree i and factor ρ^κ and isobaric functions of degree i and weight $\frac{1}{2}(ip-\kappa)$. The number of the asyzygetic invariants is then the number of partitions denoted by

$$\left(\frac{ip-\kappa}{2};\ i,p\right) = \left(\frac{ip+\kappa}{2};\ i,p\right). \tag{23}$$

The number of factor $\rho^{-\kappa}$ is the same. There is also the law of reciprocity that the number of orthogonal invariants of degree i and factor ρ^κ of a p-ic is equal to the number of degree p and factor ρ^κ of an i-ic.

The facts may also be exhibited by generating functions. Thus the *real* generating function for orthogonal invariants of a p-ic, each affected with the appropriate factor of its expression of invariancy, is

$$\left\{(1-I_p\rho^p)(1-I_{p-2}\rho^{p-2})\,\ldots\,(1-I_{-p}\rho^{-p})\right\}^{-1}. \tag{24}$$

The expansion of this in powers of ρ has for the coefficient of ρ^κ in it the sum of all the products of the I's which are the asyzygetic invariants of factor ρ^κ. The *numerical* generating function

$$\left\{(1-a\rho^p)(1-a\rho^{p-2})\,\ldots\,(1-a\rho^{-p})\right\}^{-1} \tag{25}$$

has for the coefficient of $a^i\rho^\kappa$ in it the number of the asyzygetic invariants of factor ρ^κ and of degree i.

For orthogonal covariants the real and numerical generating functions are in like manner

$$\left\{(1-I_p\rho^p)\,\ldots\,(1-I_{-p}\rho^{-p})(1-\xi\rho^{-1})(1-\eta\rho)\right\}^{-1}, \tag{26}$$

and

$$\left\{(1-a\rho^p)\,\ldots\,(1-a\rho^{-p})(1-x\rho^{-1})(1-x\rho)\right\}^{-1}. \tag{27}$$

A familiar method enables us to expand (25) in powers of a. Noticing that multiplying (25) by $1-a\rho^{-p}$ is equivalent to putting $a\rho^2$ for a in it and then multiplying by $1-a\rho^{p+2}$, we obtain, by equating coefficients of a^i in the two products,

$$C_i = \frac{1}{\rho^p}\,\frac{1-\rho^{2i+2p}}{1-\rho^{2i}}\,C_{i-1},$$

where C_i means the coefficient of a^i in the expansion of (25). Repeating the application of this to C_{i-1}, C_{i-2}, ..., and observing that $C_0 = 1$, we have

$$C_i = \frac{1}{\rho^{ip}}\,\frac{(1-\rho^{2i+2p})(1-\rho^{2i+2p-2})\,\ldots\,(1-\rho^{2p+2})}{(1-\rho^{2i})(1-\rho^{2i-2})\,\ldots\,(1-\rho^2)}. \tag{28}$$

Thus the number of orthogonal invariants of degree i and factor ρ^κ is the coefficient of ρ^κ in the expansion of (28).

7. *Systems of Absolute Orthogonal Invariants, &c.*

To obtain the real generating function for absolute orthogonal invariants (for direct transformations) of a p-ic, we have to extract from (24) the part free from ρ in its expansion. For absolute orthogonal covariants and invariants the like extraction from (26) has to be effected. More generally for absolute orthogonal covariants of a number of quantics in a number of cogredient pairs of variables x_1, y_1; x_2, y_2; &c., we have to extract the part free from ρ from

$$\left\{\Pi\left[(1-I_p\rho^p)\dots(1-I_{-p}\rho^{-p})\right]\Pi\left[(1-\xi\rho^{-1})(1-\eta\rho)\right]\right\}^{-1}. \tag{29}$$

As I do not know of a work or memoir to which to refer for the extractions in question, I have considered in the articles which follow a few early cases. I first consider only invariants.

8. For $p=1$, *i.e.*, for the case of $ax+by$, (24) is

$$\frac{1}{(1-I_1\rho)(1-I_{-1}\rho^{-1})};$$

and the terms free from ρ are

$$1+I_1I_{-1}+(I_1I_{-1})^2+\dots,$$

so that the real generating function for direct absolute orthogonal invariants is

$$\frac{1}{1-I_1I_{-1}}; \tag{30}$$

and

$$I_1I_{-1}\equiv a^2+b^2 \tag{31}$$

is the only irreducible absolute orthogonal invariant. It is (*cf.* § 5, end) invariant also for skew transformations.

9. For $p=2$, *i.e.*, for the quadratic $ax^2+2bxy+cy^2$, (24) is

$$\frac{1}{(1-I_2\rho^2)(1-I_0)(1-I_{-2}\rho^{-2})};$$

and the real generating function is at once

$$\frac{1}{(1-I_0)(1-I_2I_{-2})}, \tag{32}$$

so that and
$$\left.\begin{aligned} I_0 &\equiv a+c \\ I_2 I_{-2} &\equiv (a-c)^2+4b^2 \end{aligned}\right\} \qquad (33)$$

form the irreducible system. No syzygy connects them. They are invariant also for skew transformations.

10. For $p=3$, *i.e.*, for the cubic $(a, b, c, d)(x, y)^3$, (24) is
$$\frac{1}{(1-I_3\rho^3)(1-I_1\rho)(1-I_{-1}\rho^{-1})(1-I_{-3}\rho^{-3})}.$$

Now
$$\frac{1}{(1-I_3\rho^3)(1-I_{-3}\rho^{-3})} = \left\{\frac{1}{1-I_3\rho^3}+\frac{1}{1-I_{-3}\rho^{-3}}-1\right\}\frac{1}{1-I_3 I_{-3}}$$
$$= \frac{1}{1-I_3I_{-3}}\left\{1+\sum_{m=1}^{m=\infty}\left(I_3^m\rho^{3m}+I_{-3}^m\rho^{-3m}\right)\right\}$$

and
$$\frac{1}{(1-I_1\rho)(1-I_{-1}\rho^{-1})} = \frac{1}{1-I_1I_{-1}}\left\{1+\sum_{n=1}^{n=\infty}\left(I_1^n\rho^n+I_{-1}^n\rho^{-n}\right)\right\}.$$

Hence the part free from ρ in the product is
$$\frac{1}{(1-I_1I_{-1})(1-I_3I_{-3})}\left\{1+\sum_{m=1}^{m=\infty}\left(I_1^{3m}I_{-3}^m+I_{-1}^{3m}I_3^m\right)\right\}$$
$$= \frac{1}{(1-I_1I_{-1})(1-I_3I_{-3})}\left\{\frac{1}{1-I_1^3I_{-3}}+\frac{1}{1-I_{-1}^3I_3}-1\right\}$$
$$= \frac{1-I_1^3I_{-1}^3I_3I_{-3}}{(1-I_1I_{-1})(1-I_3I_{-3})(1-I_1^3I_{-3})(1-I_{-1}^3I_3)}. \qquad (34)$$

There are then four irreducible direct absolute orthogonal invariants of the cubic, which are best taken as the four real ones

$$\left.\begin{aligned} I_3I_{-3} &\equiv (a-3c)^2+(3b-d)^2, \\ I_1I_{-1} &\equiv (a+c)^2+(b+d)^2, \\ \tfrac{1}{2}\left\{I_3I_{-1}^3+I_{-3}I_1^3\right\} &\equiv (a+c)(a-3c)\left\{(a+c)^2-3(b+d)^2\right\} \\ &\qquad +(b+d)(3b-d)\left\{3(a+c)^2-(b+d)^2\right\}, \\ -\frac{1}{2i}\left\{I_3I_{-1}^3-I_{-3}I_1^3\right\} &\equiv (a+c)(3b-d)\left\{(a+c)^2-3(b+d)^2\right\} \\ &\qquad -(a-3c)(b+d)\left\{3(a+c)^2-(b+d)^2\right\}. \end{aligned}\right\} \qquad (35)$$

They are, by the numerator of (34), connected by one syzygy of degree 8, which expresses the sum of the squares of the last two as the product of the first and the cube of the second. For skew transformations they are also invariant by § 5, the first three being absolute, and the last having the factor -1.

The numerical generating function is

$$\frac{1-a^8}{(1-a^2)^2(1-a^4)^2}=\frac{1+a^4}{(1-a^2)^2(1-a^4)}. \tag{36}$$

11. For $p=4$, *i.e.*, for the quartic $(a, b, c, d, e)(x, y)^4$, (24) is

$$\frac{1}{(1-I_4\rho^4)(1-I_2\rho^2)(1-I_0)(1-I_{-2}\rho^{-2})(1-I_{-4}\rho^{-4})},$$

in which put z for ρ^2.

Now, just as before,

$$\frac{1}{(1-I_4z^2)(1-I_{-4}z^{-2})}=\frac{1}{1-I_4I_{-4}}\left\{1+\sum_{m=1}^{m=\infty}(I_4^mz^{2m}+I_{-4}^mz^{-2m})\right\}$$

and $$\frac{1}{(1-I_2z)(1-I_{-2}z^{-1})}=\frac{1}{1-I_2I_{-2}}\left\{1+\sum_{n=1}^{n=}(I_2^nz^n+I_{-2}^nz^{-n})\right\}.$$

Hence the real generating function required is

$$\frac{1}{(1-I_4I_{-4})(1-I_2I_{-2})(1-I_0)}\left\{1+\sum_{m=1}^{m=\infty}(I_4^mI_{-2}^{2m}+I_{-4}^mI_2^{2m})\right\}$$

$$=\frac{1-I_4I_{-4}I_2^2I_{-2}^2}{(1-I_4I_{-4})(1-I_2I_{-2})(1-I_0)(1-I_4I_{-2}^2)(1-I_{-4}I_2^2)}. \tag{37}$$

The irreducible system for the quartic accordingly consists of five invariants, best written

$$\left.\begin{aligned}
I_4I_{-4} &\equiv (a-6c+e)^2+16\,(b-d)^2,\\
I_2I_{-2} &\equiv (a-e)^2+4\,(b+d)^2,\\
I_0 &\equiv a+2c+e,\\
\tfrac{1}{2}\left\{I_4I_{-2}^2+I_{-4}I^2\right\} &\equiv (a-6c+e)\left\{(a-e)^2-4\,(b+d)^2\right\}\\
&\qquad\qquad +16\,(a-e)(b^2-d^2),\\
\frac{1}{8\iota}\left\{I_4I_{-2}^2-I_{-4}I_2^2\right\} &\equiv (a-6c+e)(a-e)(b+d)\\
&\qquad\qquad -(b-d)\left\{(a-e)^2-4\,(b+d)^2\right\}.
\end{aligned}\right\} \tag{38}$$

We are also told by (37) that these are connected by one syzygy of degree 6, which expresses the sum of the squares of the fourth and four times the fifth as the product of the first and the square of the second.

All but the last are absolute also for skew transformations. For such the last has the factor -1.

The numerical generating function is

$$\frac{1-a^6}{(1-a)(1-a^2)^2(1-a^3)^2}=\frac{1+a^3}{(1-a)(1-a^2)^2(1-a^3)}. \tag{39}$$

12. For $p=5$, *i.e.*, for the quintic, (24) is

$$\frac{1}{(1-A\rho^5)(1-B\rho^3)(1-C\rho)(1-C'\rho^{-1})(1-B'\rho^{-3})(1-A'\rho^{-5})},$$

where, for temporary convenience, we have altered the notation.

Now

$$\frac{1}{(1-A\rho^5)(1-A'\rho^{-5})}=\frac{1}{1-AA'}\left\{1+\sum_{l=1}^{l=\infty}A^l\rho^{5l}+\sum_{l'=1}^{l'=\infty}A'^{l'}\rho^{-5l'}\right\},$$

$$\frac{1}{(1-B\rho^3)(1-B'\rho^{-3})}=\frac{1}{1-BB'}\left\{1+\sum_{m=1}^{m=\infty}B^m\rho^{3m}+\sum_{m'=1}^{m'=\infty}B'^{m'}\rho^{-3m'}\right\},$$

$$\frac{1}{(1-C\rho)(1-C'\rho^{-1})}=\frac{1}{1-CC'}\left\{1+\sum_{n=1}^{n=\infty}C^n\rho^n+\sum_{n'=1}^{n'=\infty}C'^{n'}\rho^{-n'}\right\}.$$

In the product of the three expansions no term can contain both A and A', or both B and B', or both C and C'. The real generating function for absolute invariants which is required, *i.e.*, the expression whose expansion is the sum of the terms free from ρ in the product of the three right-hand members, will then be the expression for

$$\begin{aligned}\frac{1}{(1-AA')(1-BB')(1-CC')}\Bigg\{1&+\sum_{5l+3m=n'}A^lB^mC'^{n'}+\sum_{5l'+3m'=n}A'^{l'}B'^{m'}C^n\\&+\sum_{3m+n=5l'}B^mC^nA'^{l'}+\sum_{3m'+n'=5l}B'^{m'}C'^{n'}A^l\\&+\sum_{n+5l=3m'}C^nA^lB'^{m'}+\sum_{n'+5l'=3m}C'^{n'}A'^{l'}B^m\\&-\sum_{m=1}^{m=\infty}B^mC'^{3m}-\sum_{n=1}^{n=\infty}C^{5n}A'^n-\sum_{r=1}^{r=\infty}A^{3r}B'^{5r}\\&-\sum_{m=1}^{m=\infty}B'^mC^{3m}-\sum_{n=1}^{n=\infty}C'^{5n}A^n-\sum_{r=1}^{r=\infty}A'^{3r}B^{5r}\Bigg\},\end{aligned} \tag{40}$$

in which the last six sums are subtracted because each is reckoned in two previous sums. Simultaneous zero indices in any term of a sum are excluded.

Now the simple sets of positive integral solutions of

$$5l+3m = n'$$

are $\qquad 1 \quad 0 \quad 5$

and $\qquad 0 \quad 1 \quad 3.$

All other sets of solutions are sums of multiples of these sets. Hence

$$\left.\begin{array}{l} \displaystyle\sum_{5l+3m=n'} A^l B^m C'^{n'} = \sum_{r+s=1}^{r=\infty,\, s=\infty} (AC'^5)^r (BC'^3)^s \\ \displaystyle\qquad\qquad = \frac{1}{(1-AC'^5)(1-BC'^3)} -1, \\ \text{and similarly} \\ \displaystyle\sum_{5l'+3m'=n} A'^{l'} B'^{m'} C^n = \frac{1}{(1-A'C^5)(1-B'C^3)} -1. \end{array}\right\} \qquad (41)$$

Again, the simple sets of solutions of

$$3m+n = 5l'$$

are

$$\begin{array}{llll} (a) & 0 & 5 & 1, \\ (b) & 5 & 0 & 3, \\ (c) & 1 & 2 & 1, \\ (d) & 3 & 1 & 2, \end{array}$$

which are connected by the two irreducible syzygies

$$(a)+(d) \equiv 3\,(c),$$

$$(b)+(c) \equiv 2\,(d),$$

all other syzygies being, in fact, consequences of these, for instance,

$$(a)+(b) \equiv 2\,(c)+(d).$$

The justification of these statements is involved in what follows.

We proceed to see that every set of solutions of $3m+n = 5l'$ is included once in the systems of sets

$$s\,(c)+t\,(d), \quad q\,(a)+s\,(c), \quad r\,(b)+t\,(d),$$

for positive integral (not both zero) values of the multipliers, and that all sets are included once only, except sets $s\,(c)$, $t\,(d)$, which occur twice.

That every set $\qquad q\,(a)+r\,(b)+s\,(c)+t\,(d)$

can be expressed in one of the three forms is clear, because by use of $(a)+(b) \equiv 2(c)+(d)$ it can be given one of the forms

$$q(a)+s(c)+t(d), \quad r(b)+s(c)+t(d),$$

and by use of $(a)+(d) \equiv 3(c)$ the first of these can be given one of the forms $q(a)+s(c)$, $s(c)+t(d)$, and by use of $(b)+(c) \equiv 2(d)$ the second can be given one of the forms $r(b)+t(d)$, $s(c)+t(d)$.

Can, however, any set of solutions be more than once included in the three systems? It cannot be twice included in either one of the three; if, for instance, $s(c)+t(d)$ and $s'(c)+t'(d)$ were the same, we should have $s+3t = s'+3t'$ and $2s+t = 2s'+t'$, *i.e.*, $s = s'$ and $t = t'$. Neither can it be included in two different systems, unless it be of one of the forms $s(c)$, $t(d)$, which occur in two. If, for instance, we could have $s(c)+t(d)$ identical with $q'(a)+s'(c)$, we should have satisfied

$$s+3t = s', \quad 2s+t = 5q'+2s';$$

whence

$$5q' = -5t,$$

which would have to be negative unless $t = 0$. In like manner the identity of $s(c)+t(d)$ and $r'(b)+t'(d)$ would necessitate

$$s+3t = 5r'+3t', \quad 2s+t = t';$$

whence

$$5r' = -5s,$$

negative unless $s = 0$. And finally the identity of $q(a)+s(c)$ and $r'(b)+t'(d)$ would necessitate

$$s = 5r'+3t', \quad 5q+2s = t';$$

whence

$$5r' = -15q-5s,$$

which is negative.

Accordingly we have

$$\sum_{3m+n=5l'} B^m C^n A'^{l'} \text{ (in which terms with one of } m,\ n \text{ zero are included)}$$

$$= \Sigma (BC^2A')^s (B^3CA'^2)^t + \Sigma (C^5A')^q (BC^2A')^s + \Sigma (B^5A'^3)^r (B^3CA'^2)^t$$
$$- \Sigma (BC^2A')^s - \Sigma (B^3CA'^2)^t$$

$$= \frac{1}{(1-BC^2A')(1-B^3CA'^2)} + \frac{1}{(1-C^5A')(1-BC^2A')}$$
$$+ \frac{1}{(1-B^5A'^3)(1-B^3CA'^2)}$$
$$- \frac{1}{1-BC^2A'} - \frac{1}{1-B^3CA'^2} - 1$$

$$= \frac{1}{(1-BC^2A')(1-B^3CA'^2)} + \frac{C^5A'}{(1-C^5A')(1-BC^2A')}$$
$$+ \frac{B^5A'^3}{(1-B^5A'^3)(1-B^3CA'^2)} - 1. \qquad (42)$$

Similarly for the fourth summation in (40).

Once more, the simple solutions of

$$n+5l = 3m'$$

are

$$\begin{array}{cccc} (\alpha) & 3 & 0 & 1, \\ (\beta) & 0 & 3 & 5, \\ (\gamma) & 1 & 1 & 2, \end{array}$$

connected by the one syzygy

$$(\alpha)+(\beta) \equiv 3(\gamma),$$

so that all solutions are once included in

$$q(\alpha)+r(\beta)+s(\gamma),$$

with s equal to 0 or 1 or 2. Thus

$$\sum_{n+5l=3m'} C^nA^lB'^{m'} = \{1+\Sigma(C^3B')^q(A^3B'^5)^r\}\{1+CAB'^2+(CAB'^2)^2\}-1$$
$$= \frac{1-(CAB'^2)^3}{(1-C^3B')(1-A^3B'^5)(1-CAB'^2)} - 1; \qquad (43)$$

and similarly for the sixth summation in (40).

The subtracted sums in (40) amount to

$$-6+\frac{1}{1-BC'^3}+\frac{1}{1-B'C^3}+\frac{1}{1-C^5A'}+\frac{1}{1-C'^5A}+\frac{1}{1-A^3B'^5}+\frac{1}{1-A'^3B^5}. \qquad (44)$$

Consequently the desired real generating function is given by (40) in the form

$$\frac{1}{(1-AA')(1-BB')(1-CC')}$$
$$\left\{1+\frac{1}{(1-AC'^5)(1-BC'^3)}+\frac{1}{(1-A'C^5)(1-B'C^3)}\right.$$
$$+\frac{1}{(1-BC^2A')(1-B^3CA'^2)}+\frac{1}{(1-B'C'^2A)(1-B'^3C'A^2)}$$
$$+\frac{B^5A'^3}{(1-B^5A'^3)(1-B^3CA'^2)}+\frac{B'^5A^3}{(1-B'^5A^3)(1-B'^3C'A^2)}$$

$$\left. + \frac{C'^5A}{(1-C'^5A)(1-B'C'^2A)} + \frac{C^5A'}{(1-C^5A')(1-BC^2A')} \right.$$

$$+ \frac{1-(CAB'^2)^3}{(1-C^3B')(1-A^3B'^5)(1-CAB'^2)}$$

$$+ \frac{1-(C'A'B^2)^3}{(1-C'^3B)(1-A'^3B^5)(1-C'A'B^2)} - \frac{1}{1-BC'^3} - \frac{1}{1-B'C^3}$$

$$\left. - \frac{1}{1-C^5A'} - \frac{1}{1-C'^5A} - \frac{1}{1-A^3B'^5} - \frac{1}{1-A'^3B^5} \right\}. \tag{45}$$

This real generating function is readily written as one fraction, not in its lowest terms, with denominator

$$\begin{aligned} &(1-AA')(1-BB')(1-CC')(1-AC'^5)(1-A'C^5)(1-BC'^3)(1-B'C^3) \\ &\quad \times (1-A^3B'^5)(1-A'^3B^5)(1-AB'C'^2)(1-A'BC^2)(1-A^2B'^3C') \\ &\quad \times (1-A'^2B^3C)(1-AB'^2C)(1-A'B^2C'); \end{aligned} \tag{46}$$

and, from the examination above of the critical diophantine equations for their simple sets of solutions, it follows that there are no irreducible products of the absolute class which are still unrepresented in this denominator. Thus, reverting to our ordinary notation, the irreducible absolute system for the quintic consists of the fifteen orthogonal invariants

$$\left. \begin{array}{cccccc} & & I_5 I_{-5}, & I_3 I_{-3}, & I_1 I_{-1}; & \\ I_5 I_{-1}^5, & I_3 I_{-1}^3, & I_5^3 I_{-3}^5, & I_5 I_{-3} I_{-1}^2, & I_5 I_1 I_{-3}^2, & I_5^2 I_{-3}^3 I_{-1}; \\ I_{-5} I_1^5, & I_{-3} I_1^3, & I_{-5}^3 I_3^5, & I_{-5} I_5 I_1^2, & I_{-5} I_{-1} I_3^2, & I_{-5}^2 I_3^3 I_1. \end{array} \right\} \tag{47}$$

After the first three they go in conjugate pairs. Each pair is better replaced by half the sum and $\frac{1}{2\iota}$ times the difference of the pair, the whole system being thus given reality of form and applicability to skew transformations.

Three of the fifteen are of degree 2, six of degree 4, four of degree 6, and two of degree 8.

The syzygies among the fifteen would be revealed by a study of the numerator when (45) is written as one fraction with (46) for denominator.

The *numerical* generating function, obtained by putting a for each letter, accented as well as unaccented, in (45), is

$$\frac{1}{(1-a^2)^3}\left\{1+\frac{4+2a^6}{(1-a^4)(1-a^6)}+\frac{2a^8}{(1-a^6)(1-a^8)}+\frac{2-2a^{12}}{(1-a^4)^2(1-a^8)}\right.$$
$$\left.-\frac{2}{1-a^4}-\frac{2}{1-a^6}-\frac{2}{1-a^8}\right\}$$
$$=\frac{1+a^2+6a^4+9a^6+12a^8+9a^{10}+6a^{12}+a^{14}+a^{16}}{(1-a^2)^2(1-a^4)(1-a^6)(1-a^8)}, \qquad (48)$$

which is easily expanded; and the number of distinct absolute orthogonal invariants of any degree i is given as the coefficient of a^i in the expansion.

If (48) be written with denominator

$$(1-a^2)^3(1-a^4)^6(1-a^6)^4(1-a^8)^2,$$

in which all the irreducible products (47) are represented, we find that the numerator is

$$1-13a^8-18a^{10}+16a^{12}+76a^{14}+66a^{16}-76a^{18}-208a^{20}-130a^{22}+157a^{24}$$
$$+356a^{26}+192a^{28}-208a^{30}-422a^{32}-208a^{34}+192a^{36}+356a^{38}+157a^{40}$$
$$-130a^{42}-208a^{44}-76a^{46}+66a^{48}+76a^{50}+16a^{52}-18a^{54}-13a^{56}+a^{64}. \qquad (49)$$

Thus the lowest syzygies are of degree 8, of which degree there is also a "ground-form," and are thirteen in number. It will be found that they express in two ways, in terms of the irreducible products of (46) or (47), the thirteen products which consist of

$$BB'C^3C'^3,\ AA'B^2B'^2CC',\ AA'BB'C^2C'^2,\ ABB'^2CC'^3,\ A'B^2C^2C'^3,$$
$$ABB'C'^5,\ AA'BB'^2C^3,\ A^2B'^3CC'^2, \qquad (50)$$

and the results of interchanging accented and unaccented letters in the last five. Of degree 10, besides the products of these syzygies of degree 8 and AA', BB', CC', there are eighteen further syzygies. These are found to express in two ways the nine products

$$AB'C^3C'^5,\ A^2B'^2CC'^5,\ AA'B^2C'^6,\ AA'BC^2C'^5,\ A'^2B^4CC'^3,\ A'^2B^3B'C^4,$$
$$AA'^2B^3B'^2C^2,\ A'^3B^5CC',\ AA'^2B^3B'CC'^2, \qquad (51)$$

and the results of interchanging accented and unaccented letters in them. As to products of the next degree 12, the number of distinct ones is sixteen more than the result of subtracting from the number of products of degree 12, formed out of (47), thirteen times the number of degree 4 and eighteen times the number of degree 2, because many will have been subtracted more than once because of syzygies (50) and (51); and so on.

13. For $p = 6$, *i.e.*, for the sextic, the analysis is somewhat simpler than for the quintic. Putting z for ρ^2, and changing the notation, (24) is now

$$\frac{1}{(1-Iz^3)(1-Jz^2)(1-Kz)(1-L)(1-K'z^{-1})(1-J'z^{-2})(1-I'z^{-3})}.$$

Now
$$\frac{1}{(1-Iz^3)(1-I'z^{-3})} = \frac{1}{1-II'}\left\{1+\sum_{l=1}^{l=\infty} I^l z^{3l} + \sum_{l'=1}^{l'=\infty} I'^{l'} z^{-3l'}\right\},$$

$$\frac{1}{(1-Jz^2)(1-J'z^{-2})} = \frac{1}{1-JJ'}\left\{1+\sum_{m=1}^{m=\infty} J^m z^{2m} + \sum_{m'=1}^{m'=\infty} J'^{m'} z^{-2m'}\right\},$$

$$\frac{1}{(1-Kz)(1-K'z^{-1})} = \frac{1}{1-KK'}\left\{1+\sum_{n=1}^{n=\infty} K^n z^n + \sum_{n'=1}^{n'=} K'^{n'} z^{-n'}\right\}.$$

The real generating function required is then the expression for

$$\begin{aligned}\frac{1}{(1-II')(1-JJ')(1-KK')(1-L)} & \\ \Big\{1 &+ \sum_{3l+2m=n'} I^l J^m K'^{n'} + \sum_{3l'+2m'=n} I'^{l'} J'^{m'} K^n \\ &+ \sum_{2m+n=3l'} J^m K^n I'^{l'} + \sum_{2m'+n'=3l} J'^{m'} K'^{n'} I^l \\ &+ \sum_{n+3l=2m'} K^n I^l J'^{m'} + \sum_{n'+3l'=2m} K'^{n'} I'^{l'} J^m \\ &- \sum_{m=1}^{m=\infty} J^m K'^{2m} - \sum_{l=1}^{l=\infty} K^{3l} I'^l - \sum_{n=1}^{n=\infty} I^{2n} J'^{3n} \\ &- \sum_{m=1}^{m=\infty} J'^m K^{2m} - \sum_{l=1}^{l=\infty} K'^{3l} I^l - \sum_{n=1}^{n=\infty} I'^{2n} J^{3n}\Big\},\end{aligned} \tag{52}$$

the last six sums being subtracted because they have been reckoned twice in previous sums.

The simple sets of solutions of

$$3l+2m = n'$$

are $\quad 1 \quad 0 \quad 3$

and $\quad 0 \quad 1 \quad 2.$

Hence
$$\begin{aligned}\sum_{3l+2m=n'} I^l J^m K'^{n'} &= \sum_{l+m=1}^{l=\infty,\, m=\infty} (IK'^3)^l\,(JK'^2)^m \\ &= \frac{1}{(1-IK'^3)(1-JK'^2)} - 1\end{aligned} \tag{53}$$

and similarly for the second summation in (52).

Again, the simple sets of solutions of

$$2m+n = 3l'$$

are

$$\begin{array}{cccc} (a) & 3 & 0 & 2, \\ (b) & 0 & 3 & 1, \\ (c) & 1 & 1 & 1, \end{array}$$

which are connected by the syzygy

$$(a)+(b) \equiv 3\,(c).$$

Every set of solutions is then included once and once only in the set

$$q\,(a)+r\,(b)+s\,(c),$$

with $q+r+s \geqq 1$ and $s = 0$ or 1 or 2. Hence

$$\sum_{2m+n=3l'} J^m K^n I'^{l'} = \left\{1+\sum_{m+n=1}^{m=\infty,\,n=\infty} (J^3I'^2)^m\,(K^3I')^n\right\}\{1+JKI'+(JKI')^2\}-1$$

$$= \frac{1-(JKI')^3}{(1-J^3I'^2)(1-K^3I')(1-JKI')}-1\,; \tag{54}$$

and similarly for the fourth summation in (52).

Once more the simple sets of solutions of

$$n+3l = 2m'$$

are

$$\begin{array}{cccc} (\alpha) & 2 & 0 & 1, \\ (\beta) & 0 & 2 & 3, \\ (\gamma) & 1 & 1 & 2, \end{array}$$

with the one syzygy $\quad (\alpha)+(\beta) \equiv 2\,(\gamma).$

The form which includes every set of solutions once is then

$$q\,(\alpha)+r\,(\beta)+s\,(\gamma),$$

with $q+r+s \geqq 1$ and $s = 0$ or 1. Consequently

$$\sum_{n+3l=2m'} K^n I^l J'^{m'} = \left\{1+\sum_{n+l=1}^{n=\infty,\,l=\infty} (K^2J')^n\,(I^2J'^3)^l\right\}(1+KIJ'^2)-1$$

$$= \frac{1-(KIJ'^2)^2}{(1-K^2J')(1-I^2J'^3)(1-KIJ'^2)}-1\,; \tag{55}$$

and similarly for the sixth summation.

The seventh to twelfth summations in (52) are at once performed;

and we thus arrive at our desired real generating function, the equivalent of (52), in the form

$$
\begin{aligned}
&\frac{1}{(1-II')(1-JJ')(1-KK')(1-L)} \\
&\left\{1+\frac{1}{(1-IK'^3)(1-JK'^2)}+\frac{1}{(1-I'K^3)(1-J'K^2)}\right. \\
&\quad +\frac{1-(I'JK)^3}{(1-I'^2J^3)(1-I'K^3)(1-I'JK)}+\frac{1-(IJ'K')^3}{(1-I^2J'^3)(1-IK'^3)(1-IJ'K')} \\
&\quad +\frac{1-(IJ'^2K)^2}{(1-J'K^2)(1-I^2J'^3)(1-IJ'^2K)}+\frac{1-(I'J^2K')^2}{(1-JK'^2)(1-I'^2J^3)(1-I'J^2K')} \\
&\quad \left.-\frac{1}{1-JK'^2}-\frac{1}{1-J'K^2}-\frac{1}{1-I'K^3}-\frac{1}{1-IK'^3}-\frac{1}{1-I^2J'^3}-\frac{1}{1-I'^2J^3}\right\}.
\end{aligned}
\tag{56}
$$

It may be written as one fraction, not in its lowest terms, with the denominator

$$
\begin{aligned}
(1-L)(1-II')(1-JJ')(1-KK')(1-JK'^2)(1-J'K^2)(1-IJ'K') \\
\times(1-I'JK)(1-IK'^3)(1-I'K^3)(1-IJ'^2K)(1-I'J^2K') \\
\times(1-I^2J'^3)(1-I'^2J^3)\,;
\end{aligned}
$$

and in this denominator all the irreducible products which are absolute orthogonal invariants occur. There are altogether fourteen in the irreducible system, namely, in our old notation,

$$
\left.
\begin{array}{ll}
\text{one linear} & I_0, \\
\text{three quadratic} & I_6I_{-6},\ I_4I_{-4},\ I_2I_{-2}, \\
\text{four cubic} & I_4I_{-2}^2,\ I_{-4}I_2^2;\ I_6I_{-4}I_{-2},\ I_{-6}I_4I_2, \\
\text{four quartic} & I_6I_{-2}^3,\ I_{-6}I_2^3;\ I_6I_{-4}^2I_2,\ I_{-6}I_4^2I_{-2}, \\
\text{and two quintic} & I_6^2I_{-4}^3,\ I_{-6}^2I_4^3.
\end{array}
\right\}
\tag{57}
$$

After the first four they go in conjugate pairs, and each pair is better replaced by the equivalent pair of real forms obtained by taking half the sum and $\frac{1}{2\iota}$ times the difference of the two.

The numerical generating function is

$$
\frac{1}{(1-a)(1-a^2)^3}\left\{1+\frac{2}{(1-a^3)(1-a^4)}+\frac{4-2a^8-2a^9}{(1-a^3)(1-a^4)(1-a^5)}\right.
$$
$$
\left.-\frac{2}{1-a^3}-\frac{2}{1-a^4}-\frac{2}{1-a^5}\right\}
$$

$$\equiv \frac{1+a^2+3a^3+4a^4+4a^5+4a^6+3a^7+a^8+a^{10}}{(1-a)(1-a^2)^2(1-a^3)(1-a^4)(1-a^5)}$$

$$\begin{aligned}\equiv \{&1-6a^6-10a^7-12a^8+2a^9+29a^{10}+48a^{11}+41a^{12}-6a^{13}-66a^{14}\\ &-102a^{15}-77a^{16}+4a^{17}+90a^{18}+128a^{19}+90a^{20}+4a^{21}-77a^{22}\\ &-102a^{23}-66a^{24}-6a^{25}+41a^{26}+48a^{27}+29a^{28}+2a^{29}-12a^{30}-10a^{31}\\ &-6a^{32}+a^{33}\}\\ &\div (1-a)(1-a^2)^3(1-a^3)^4(1-a^4)^4(1-a^5)^2. \qquad (58)\end{aligned}$$

In the last form of this all of the irreducible systems are represented in the denominator. The numerator gives information as to the syzygies. Thus the lowest syzygies are of degree 6, and are six in number. They are at once seen to be

$$\left.\begin{aligned} I_4I_{-2}^2\,.\,I_{-4}I_2^2 &\equiv I_4I_{-4}\,.\,(I_2I_{-2})^2,\\ I_6I_{-4}I_{-2}\,.\,I_{-6}I_4I_2 &\equiv I_6I_{-6}\,.\,I_4I_{-4}\,.\,I_2I_{-2},\\ I_4I_{-2}^2\,.\,I_6I_{-4}I_{-2} &\equiv I_4I_{-4}\,.\,I_6I_{-2}^3,\\ I_4I_{-2}^2\,.\,I_{-6}I_4I_2 &\equiv I_2I_{-2}\,.\,I_{-6}I_4^2I_{-2}, \end{aligned}\right\} \qquad (59)$$

and the results of changing the signs of the suffixes in the last two. Again, the term $-10a^7$ in the numerator tells us that besides I_0 times (59) there are ten new syzygies of degree 7. These give other expressions for the five products

$$I_4I_{-2}^2\,.\,I_{-6}I_2^3,\quad I_4I_{-2}^2\,.\,I_6I_{-4}^2I_2,\quad I_6I_{-4}I_{-2}\,.\,I_{-6}I_4^2I_{-2},$$
$$I_6I_{-4}I_{-2}\,.\,I_{-6}I_2^3,\quad I_6I_{-4}I_{-2}\,.\,I_6I_{-4}^2I_2, \qquad (60)$$

and their five conjugates; and so on.

14. *Absolute Orthogonal Invariants for Systems of Quantics.*

It will, I have no doubt, suffice to write down the other results at which I have arrived without exhibiting the tedious, but not difficult, calculations. No complication of a kind not already sufficiently exemplified arises.

I use R.G.F. and N.G.F. to denote respectively real and numerical generating functions, and A.O.I. and A.O.C. for absolute orthogonal invariants and covariants (including invariants) respectively.

(A) *Two linear forms* $ax+by$, $a'x+b'y$. — For this system the R.G.F. A.O.I. is

$$\frac{1-I_1I_{-1}J_1J_{-1}}{(1-I_1I_{-1})(1-J_1J_{-1})(1-I_1J_{-1})(1-I_{-1}J_1)},$$

where I_1, I_{-1} and J_1, J_{-1} are the fundamental linear orthogonal invariants of the two forms respectively. The irreducible system of A.O.I.'s consists then of the four invariants

$$\begin{aligned} I_1I_{-1} &\equiv a^2+b^2, \\ J_1J_{-1} &\equiv a'^2+b'^2, \\ \tfrac{1}{2}\{I_1J_{-1}+I_{-1}J_1\} &\equiv aa'+bb', \\ \frac{1}{2i}\{I_1J_{-1}-I_{-1}J_1\} &\equiv ab'-a'b, \end{aligned}$$

connected by the one syzygy

$$(a^2+b^2)(a'^2+b'^2) = (aa'+bb')^2+(ab'-a'b)^2.$$

(B) *Three linear forms.*—If I_1, I_{-1}; J_1, J_{-1}; K_1, K_{-1} refer to the three forms, the R.G.F. A.O.I. is

$$\frac{1}{(1-I_1I_{-1})(1-J_1J_{-1})(1-K_1K_{-1})}$$

$$\left\{1+\frac{J_1K_{-1}}{(1-I_1K_{-1})(1-J_1K_{-1})}+\frac{J_{-1}K_1}{(1-I_{-1}K_1)(1-J_{-1}K_1)}\right.$$
$$+\frac{I_1J_{-1}}{(1-J_{-1}K_1)(1-I_1J_{-1})}+\frac{I_{-1}J_1}{(1-J_1K_{-1})(1-I_{-1}J_1)}$$
$$\left.+\frac{I_1K_{-1}}{(1-I_1J_{-1})(1-I_1K_{-1})}+\frac{I_{-1}K_1}{(1-I_{-1}J_1)(1-I_{-1}K_1)}\right\}.$$

The N.G.F. is, if a, a', a'' refer to the three forms,

$$\frac{1+\Sigma aa'-aa'a''\Sigma a-a^2a'^2a''^2}{(1-a^2)(1-a'^2)(1-a''^2)(1-aa')(1-aa'')(1-a'a'')},$$

or, if we do not distinguish between degrees in the different pairs of coefficients,

$$\frac{1+4a^2+a^4}{(1-a^2)^6} \equiv \frac{1-9a^4+16a^6-9a^8+a^{12}}{(1-a^2)^9}.$$

There are nine invariants in the irreducible system, three of each of the types

$$a^2+b^2,\quad aa'+bb',\quad ab'-a'b,$$

no new type occurring which did not present itself in the case of two linear forms. (We readily convince ourselves that no new type occurs for any greater number of linear forms.)

The lowest syzygies are of degree 4 and are nine in number. There are three of each of the types

$$I_1I_{-1}.J_1J_{-1} \equiv I_1J_{-1}.I_{-1}J_1,\quad I_1I_{-1}.J_1K_{-1} \equiv I_1K_{-1}.I_{-1}J_1,$$
$$I_1I_{-1}.J_{-1}K_1 \equiv I_1J_{-1}.I_{-1}K_1.$$

The next coefficient 16 in the numerator of the last written form of the N.G.F. is positive. The new syzygies (if there be any) of degree 6 are then less in number by sixteen than the number of times we subtract products of degree 6 from the whole number of products of degree 6 which are obtained as products of three of the nine irreducible products of degree 2, when we take away the number of products of syzygies of degree 4 and the products of degree 2. For instance,

$$I_1I_{-1}J_1J_{-1}K_1K_{-1},$$

which must have coefficient 1 in the expansion of the R.G.F., is reckoned six times as a product of three of I_1I_{-1}, I_1J_{-1}, ..., is taken away nine times, once because of each of the syzygies of degree 4, and has accordingly to be reckoned four times more.

(C) *Quadratic and linear form.*—If I_2, I_0, I_{-2} and J_1, J_{-1} refer to the two forms, the R.G.F. A.O.I. is

$$\frac{1-I_2I_{-2}J_1^2J_{-1}^2}{(1-I_0)(1-I_2I_{-2})(1-J_1J_{-1})(1-I_2J_{-1}^2)(1-I_{-2}J_1^2)}.$$

There is then one syzygy of partial degrees 2, 4 among a system of five irreducible invariants. The five are, if we take half the sum and $\frac{1}{4\iota}$ times the difference of the conjugate pair, the two of the quadratic

$$a+c,\quad (a-c)^2+4b^2,$$

the one of the linear form $a'^2+b'^2$,

and the two

$$(a-c)(a'^2-b'^2)+4ba'b',\quad (a-c)\,a'b'-b\,(a'^2-b'^2).$$

(D) *Quadratic and two linear forms.*—If I_2, I_0, I_{-2}; J_1, J_{-1}; K_1, K_{-1} refer to the forms respectively, the R.G.F. A.O.I. is

$$\frac{1}{(1-I_0)(1-I_2I_{-2})(1-J_1J_{-1})(1-K_1K_{-1})}$$

$$\left\{1+\frac{J_1K_{-1}}{(1-I_2K_{-1}^2)(1-J_1K_{-1})}+\frac{J_{-1}K_1}{(1-I_{-2}K_1^2)(1-J_{-1}K_1)}\right.$$

$$+\frac{J_{-1}K_1}{(1-I_2J_{-1}^2)(1-J_{-1}K_1)}+\frac{J_1K_{-1}}{(1-I_{-2}J_1^2)(1-J_1K_{-1})}$$

$$+\frac{1-(I_{-2}J_1K_1)^2}{(1-I_{-2}J_1^2)(1-I_{-2}K_1^2)(1-I_{-2}J_1K_1)}$$

$$+\frac{1-(I_2J_{-1}K_{-1})^2}{(1-I_2J_{-1}^2)(1-I_2K_{-1}^2)(1-I_2J_{-1}K_{-1})}$$

$$\left.-\frac{1}{1-J_1K_{-1}}-\frac{1}{1-J_{-1}K_1}\right\}.$$

The irreducible system consists of the twelve forms

$$I_0,\quad I_2I_{-2},\quad J_1J_{-1},\quad K_1K_{-1},\quad J_1K_{-1}\pm J_{-1}K_1,\quad I_2J_{-1}^2\pm I_{-2}J_1^2,$$

$$I_2K_{-1}^2\pm I_{-2}K_1^2,\quad I_2J_{-1}K_{-1}\pm I_{-2}J_1K_1.$$

Eight of them are of types such as occur in (C), and the remaining four are

$$a'a''+b'b'',\quad a'b''-a''b',$$

$$(a-c)(a'a''-b'b'')+2b\,(a'b''+a''b'),$$

$$(a-c)(a'b''+a''b')-2b\,(a'a''-b'b'').$$

(E) *Two quadratics.*—The R.G.F. A.O.I. is

$$\frac{1-I_2I_{-2}J_2J_{-2}}{(1-I_0)(1-J_0)(1-I_2I_{-2})(1-J_2J_{-2})(1-I_2J_{-2})(1-I_{-2}J_2)};$$

and the irreducible system consists of six members

$$a+c,\quad a'+c',$$

$$(a-c)^2+4b^2,\quad (a'-c')^2+4b'^2,$$

$$(a-c)(a'-c')+4bb',\quad (a-c)\,b'-b\,(a'-c'),$$

which are connected by the one syzygy of partial degrees 2, 2

$$\{(a-c)(a'-c')+4bb'\}^2+4\,\{(a-c)\,b'-b\,(a'-c')\}^2$$

$$\equiv I_2I_{-2}J_2J_{-2}$$

$$\equiv \{(a-c)^2+4b^2\}\,\{(a'-c')^2+4b'^2\}.$$

(F) *Two quadratics and linear form.*—The R.G.F. A.O.I. is

$$\frac{1}{(1-I_0)(1-J_0)(1-I_2I_{-2})(1-J_2J_{-2})(1-K_1K_{-1})}$$

$$\times\left\{1-\frac{J_2K^2_{-1}}{(1-I_2K^2_{-1})(1-J_2K^2_{-1})}+\frac{J_{-2}K_1^2}{(1-I_{-2}K_1^2)(1-J_{-2}K_1^2)}\right.$$

$$+\frac{I_2J_{-2}}{(1-J_{-2}K_1^2)(1-I_2J_{-2})}+\frac{I_{-2}J_2}{(1-J_2K^2_{-1})(1-I_{-2}J_2)}$$

$$\left.+\frac{I_2K^2_{-1}}{(1-I_2J_{-2})(1-I_2K^2_{-1})}+\frac{I_{-2}K_1^2}{(1-I_{-2}J_2)(1-I_{-2}K_1^2)}\right\};$$

and there are eleven members of the irreducible system, of seven types, viz.,

$$I_0,\quad J_0,\quad I_2I_{-2},\quad J_2J_{-2},\quad K_1K_{-1},\quad I_2J_{-2}\pm I_{-2}J_2,\quad I_2K^2_{-1}\pm I_{-2}K_1^2.$$
$$J_2K^2_{-1}\pm J_{-2}K_1^2.$$

(G) *Three quadratics.*—The R.G.F. A.O.I. is

$$\frac{1}{(1-I_0)(1-J_0)(1-K_0)(1-I_2I_{-2})(1-J_2J_{-2})(1-K_2K_{-2})}$$

$$\times\left\{1+\frac{J_2K_{-2}}{(1-I_2K_{-2})(1-J_2K_{-2})}+\frac{J_{-2}K_2}{(1-I_{-2}K_2)(1-J_{-2}K_2)}\right.$$

$$+\frac{I_2J_{-2}}{(1-J_{-2}K_2)(1-I_2J_{-2})}+\frac{I_{-2}J_2}{(I-J_2K_{-2})(1-I_{-2}J_2)}$$

$$\left.+\frac{I_2K_{-2}}{(1-I_2J_{-2})(1-I_2K_{-2})}+\frac{I_{-2}K_2}{(1-I_{-2}J_2)(1-I_{-2}K_2)}\right\}.$$

Accordingly the irreducible system consists of twelve invariants, all of types which have occurred in the system for two quadratics. It will be found that no new types occur for n quadratics.

The N.G.F. for three quadratics is that of (B) multiplied by

$$\frac{1}{(1-a)(1-a')(1-a'')}.$$

(H) *Cubic and linear form.*—The R.G.F. A.O.I. is

$$\frac{1}{(1-I_3I_{-3})(1-I_1I_{-1})(1-J_1J_{-1})}$$

$$\times\left\{1+\frac{I_1J_{-1}}{(1-I_3J^3_{-1})(1-I_1J_{-1})}+\frac{I_{-1}J_1}{(1-I_{-3}J_1^3)(1-I_{-1}J_1)}\right.$$

$$+\frac{I_{-1}J_1}{(1-I_{-1}J_1)(1-I_3I_{-1}^3)}+\frac{I_1J_{-1}}{(1-I_1J_{-1})(1-I_{-3}I_1^3)}$$

$$+\frac{1}{(1-I_{-3}I_1^2J_1)(1-I_{-3}I_1J_1^2)}+\frac{1}{(1-I_3I_{-1}^2J_{-1})(1-I_3I_{-1}J_{-1}^2)}$$

$$+\frac{I_{-1}J_1^3}{(1-I_{-3}J_1^3)(1-I_{-3}I_1J_1^2)}+\frac{I_3J_{-1}^3}{(1-I_3J_{-1}^3)(1-I_3I_{-1}J_{-1}^2)}$$

$$+\frac{I_3I_{-1}^3}{(1-I_3I_{-1}^3)(1-I_3I_{-1}^2J_{-1})}+\frac{I_{-3}I_1^3}{(1-I_{-3}I_1^3)(1-I_{-3}I_1^2J_1)}$$

$$\left.-\frac{1}{1-I_1J_{-1}}-\frac{1}{1-I_{-1}J_1}\right\}.$$

There are then thirteen members of the irreducible system, viz., the four (35) of the cubic, the one (31) of the linear form, and the four pairs

$$I_1J_{-1}\pm I_{-1}J_1,\quad I_3J_{-1}^3\pm I_{-3}J_1^3,\quad I_3I_{-1}J_{-1}^2\pm I_{-3}I_1J_1^2,\quad I_3I_{-1}^2J_{-1}\pm I_{-3}I_1^2J_1.$$

(K) *Cubic and quadratic.*—If I_3, I_1, I_{-1}, I_{-3} refer to the cubic, and J_2, J_0, J_{-2} to the quadratic, the R.G.F. A.O.I. and the irreducible system are what those, (56) and (57), for one sextic become when in them for

$$I,\ I',\ J,\ J',\ K,\ K',\ L,$$

or $$I_6,\ I_{-6},\ I_4,\ I_{-4},\ I_2,\ I_{-2},\ I_0,$$

we put $$I_3,\ I_{-3},\ J_2,\ J_{-2},\ I_1,\ I_{-1},\ J_0.$$

(L) *Quartic and linear form.*—The R.G.F. A.O.I. is

$$\frac{1}{(1-I_0)(1-I_2I_{-2})(1-I_4I_{-4})(1-J_1J_{-1})}$$

$$\times\left\{1+\frac{I_2J_{-1}^2}{(1-I_4J_{-1}^4)(1-I_2J_{-1}^2)}+\frac{I_{-2}J_1^2}{(1-I_{-4}J_1^4)(1-I_{-2}J_1^2)}\right.$$

$$+\frac{I_{-2}J_1^2}{(1-I_4I_{-2}^2)(1-I_{-2}J_1^2)}+\frac{I_2J_{-1}^2}{(1-I_{-4}I_2^2)(1-I_2J_{-1}^2)}$$

$$+\frac{1-(I_{-4}I_2J_1^2)^2}{(1-I_{-4}I_2^2)(1-I_{-4}J_1^4)(1-I_{-4}I_2J_1^2)}$$

$$+\frac{1-(I_4I_{-2}J_{-1}^2)^2}{(1-I_4I_{-2}^2)(1-I_4J_{-1}^4)(1-I_4I_{-2}J_{-1}^2)}$$

$$\left.-\frac{1}{1-I_2J_{-1}^2}-\frac{1}{1-I_{-2}J_1^2}\right\}.$$

The irreducible system consists of twelve forms, viz., the five (38) of the quartic, the one (31) of the linear form, and the three pairs

$$I_2J_{-1}^2 \pm I_{-2}J_1^2, \quad I_4I_{-2}J_{-1}^2 \pm I_{-4}I_2J_1^2, \quad I_4J_{-1}^4 \pm I_{-4}J_1^4.$$

(M) *Quartic and quadratic.*—If $I_4, I_2, I_0, I_{-2}, I_{-4}$ refer to the quartic, and J_2, J_0, J_{-2} to the quadratic, the R.G.F. A.O.I. is obtained from that of (D) for a quadratic and two linear forms by dividing by $1-J_0$, and replacing

$$I_2,\ I_0,\ I_{-2},\ J_1,\ J_{-1},\ K_1,\ K_{-1}$$

by

$$I_4,\ I_0,\ I_{-4},\ I_2,\ I_{-2},\ J_2,\ J_{-2},$$

respectively. There are thirteen invariants in the irreducible system, viz., the five (38) of the quartic, the two (33) of the quadratic, and three pairs

$$I_2J_{-2} \pm I_{-2}J_2, \quad I_4I_{-2}J_{-2} \pm I_{-4}I_2J_2, \quad I_4J_{-2}^2 \pm I_{-4}J_2^2.$$

15. It will be well to explain and generalise some coincidences in the above list. The R.G.F. A.O.I. for a quartic is of exactly the same form as that for a quadratic and a linear form. Again, that for a sextic is of the same form as that for a cubic and a quadratic. The general fact which accounts for these identities of form is that there is a complete one to one correspondence of orthogonal invariants —non-absolute as well as absolute—of a $2p$-ic with those of a p-ic and a $(p-1)$-ic jointly. In fact the one generating function is

$$\{(1-I_{2p}\rho^{2p})(1-I_{2p-2}\rho^{2p-2})\ \dots\ (1-I_{-2p+2}\rho^{-2p+2})(1-I_{-2p}\rho^{-2p})\}^{-1},$$

and the other is

$$\{(1-J_p\rho^p)(1-J_{p-2}\rho^{p-2})\ \dots\ (1-J_{-p}\rho^{-p}).(1-K_{p-1}\rho^{p-1})(1-K_{p-3}\rho^{p-3})\ \dots$$
$$\dots\ (1-K_{-p+1}\rho^{-p+1})\}^{-1}.$$

and, replacing ρ by ρ^2 in the second, it becomes the first with

$$J_p,\ K_{p-1},\ J_{p-2},\ \dots,\ J_{-p+2},\ K_{-p+1},\ J_{-p},$$

respectively, written for

$$I_{2p},\ I_{2p-2},\ I_{2p-4},\ \dots,\ I_{-2p+4},\ I_{-2p+2},\ I_{-2p}.$$

The reason is not hard to discover. If x, y are orthogonally transformed—turned through θ—so also are x^2-y^2, $2xy$—turned through 2θ. Now our $2p$-ic is (11) a numerical multiple of

$$(I_{2p},\ I_{2p-2},\ \dots,\ I_{-2p+2},\ I_{-2p})(\xi,\ \eta)^{2p},$$

i.e., of $(J'_p, J'_{p-2}, \dots, J'_{-p})(\xi^2, \eta^2)^p + \xi\eta\,(K'_{p-1}, K'_{p-3}, \dots, K'_{-p+1})(\xi^2, \eta^2)^{p-1}$,
where
$$J'_p,\ K'_{p-1},\ J'_{p-2},\ \dots,\ K'_{-p+1},\ J'_{-p}$$
are numerical multiples of
$$I_{2p},\ I_{2p-2},\ I_{2p-4},\ \dots,\ I_{-2p+2},\ I_{-2p};$$
also $\xi^2 \equiv x^2-y^2+2\iota xy$, $\eta^2 \equiv x^2-y^2-2\iota xy$, and $\xi\eta \equiv x^2+y^2$ the absolute. The J's and K's are then the fundamental linear orthogonal invariants of a p-ic and a $(p-1)$-ic in x^2-y^2, $2xy$.

16. *Systems of Absolute Orthogonal Covariants (including Invariants).*

By (26) and (29) the generating function for covariants of a given binary form, or system of forms, is the same as that for invariants of the system of forms which consists of the given form or system and a linear form whose fundamental orthogonal invariants I'_1, I'_{-1} are η, ξ respectively. Accordingly the results of § 14 also give us the following:—

(N) *System for one linear form* $ax+by$.—The R.G.F. A.O.C. is obtained by putting ξ, η for J_{-1}, J_1 in that of § 14 (A). The system consists of
$$a^2+b^2,\quad x^2+y^2,\quad ax+by,\quad ay-bx,$$
with the one syzygy
$$(a^2+b^2)(x^2+y^2) \equiv (ax+by)^2+(ay-bx)^2.$$

(P) *Two linear forms* $ax+by$, $a'x+b'y$.—The R.G.F. A.O.C. is the result of putting ξ, η for K_{-1}, K_1 in that of § 14 (B). The system consists of the four invariants of (A), the absolute x^2+y^2, and the four covariants
$$ax+by,\quad a'x+b'y,\quad ay-bx,\quad a'y-b'x.$$

(Q) *One quadratic* $(a, b, c)(x, y)^2$.—For the R.G.F. A.O.C. we put ξ, η for J_{-1}, J_1 in that of (C). There are in the irreducible system, besides the absolute x^2+y^2 and the two invariants
$$a+c,\quad (a-c)^2+4b^2,$$
the two covariants
$$(a-c)(x^2-y^2)+4bxy,\quad (a-c)\,xy-b\,(x^2-y^2).$$
The one connecting syzygy is
$$\{(a-c)^2+4b^2\}(x^2+y^2)^2 \equiv \{(a-c)(x^2-y^2)+4bxy\}^2 + 4\,\{(a-c)\,xy-b(x^2-y^2)\}^2,$$
and the N.G.F. is
$$\frac{1+ax^2}{(1-a)(1-a^2)(1-x^2)(1-ax^2)}.$$

The quadratic itself is a linear combination of the first covariant and $(a+c)(x^2+y^2)$.

(R) *Quadratic and linear form.*—For the R.G.F. A.O.C. we have to put ξ, η for K_{-1}, K_1 in the R.G.F. of (D). The irreducible system consists of the five invariants given in (C), the absolute x^2+y^2, and the six covariants

$$(a-c)(x^2-y^2)+4bxy, \quad (a-c)\,xy-b\,(x^2-y^2),$$
$$a'x+b'y, \quad b'x-a'y,$$
$$(a-c)(a'x-b'y)+2b\,(a'y+b'x), \quad (a-c)(a'y+b'x)-2b\,(a'x-b'y).$$

(S) *Two quadratics.*—The R.G.F. A.O.C. is the result of putting ξ, η for K_{-1}, K_1 in the R.G.F. of (F). There are eleven members of the irreducible system, viz., x^2+y^2, the six invariants given in (E), and the four covariants

$$(a-c)(x^2-y^2)+4bxy, \quad (a'-c')(x^2-y^2)+4b'xy,$$
$$(a-c)\,xy-b\,(x^2-y^2), \quad (a'-c')\,xy-b'(x^2-y^2).$$

The N.G.F. for the system is

$$\frac{1+aa'+(a+a')(1-aa')\,x^2-aa'x^4-a^2a'^2x^4}{(1-a)(1-a')(1-a^2)(1-a'^2)(1-aa')(1-ax^2)(1-a'x^2)(1-x^2)}.$$

(T) *One cubic* $(a,\,b,\,c,\,d)(x,\,y)^3$.—For the R.G.F. A.O.C. put ξ, η for J_{-1}, J_1 in the R.G.F. of (H).

The irreducible system consists of the absolute x^2+y^2, the four invariants of § 10, and eight covariants given by the last line of (H). Rejecting factors 2 and 2ι, these eight covariants are

$$(a+c)\,x+(b+d)\,y,$$
$$(b+d)\,x-(a+c)\,y,$$
$$(a-3c)\,x\,(x^2-3y^2)+(3b-d)\,y\,(3x^2-y^2),$$
$$(3b-d)\,x\,(x^2-3y^2)-(a-3c)\,y\,(3x^2-y^2),$$
$$\{(a+c)^2-(b+d)^2\}\{(a-3c)\,x+(3b-d)\,y\}$$
$$+2\,(a+c)(b+d)\{(3b-d)\,x-(a-3c)\,y\},$$
$$\{(a+c)^2-(b+d)^2\}\{(3b-d)\,x-(a-3c)\,y\}$$
$$-2\,(a+c)(b+d)\,\{(a-3c)\,x+(3b-d)\,y\}.$$
$$\{(a-3c)(a+c)+(3b-d)(b+d)\}\,(x^2-y^2)$$
$$+2\,\{(a+c)(3b-d)-(a-3c)(b+d)\}\,xy,$$
$$\{(a+c)(3b-d)-(a-3c)(b+d)\}(x^2-y^2)$$
$$-2\,\{(a-3c)(a+c)+(3b-d)(b+d)\}\,xy.$$

Note that the full covariant $(a^2d-3abc+2b^3)x^3+\ldots$, regarded as an absolute orthogonal covariant, is reducible in terms of the others.* With this exception the irreducible system of full covariants and invariants of a cubic and quadratic yield the equivalents of the above system upon taking the absolute x^2+y^2 for the quadratic.

(U) *One quartic* $(a, b, c, d, e)(x, y)^4$.—The R.G.F. A.O.C. is got by putting ξ, η for J_{-1}, J_1 in the R.G.F. of (L). The irreducible system consists then of x^2+y^2, the five invariants of § 11, and six covariants

$$I_2\xi^2 \pm I_{-2}\eta^2, \quad I_4 I_{-2}\xi^2 \pm I_{-4} I_2\eta^2, \quad I_4\xi^4 \pm I_{-4}\eta^4.$$

These prove to be, on rejection of powers of 2 and ι as factors,

$$(a-e)(x^2-y^2)+4(b+d)xy,$$

$$(b+d)(x^2-y^2)-(a-e)xy,$$

$$\{(a-6c+e)(a-e)+8(b^2-d^2)\}(x^2-y^2)$$
$$-4\{(a-6c+e)(b+d)-2(a-e)(b-d)\}xy,$$

$$\{(a-6c+e)(b+d)-2(a-e)(b-d)\}(x^2-y^2)$$
$$+\{(a-6c+e)(a-e)+8(b^2-d^2)\}xy,$$

$$(a-6c+e)(x^4-6x^2y^2+y^4)+16(b-d)xy(x^2-y^2),$$
$$(b-d)(x^4-6x^2y^2+y^4)-(a-6c+e)xy(x^2-y^2).$$

On some Properties of Groups of Odd Order. (Second Paper.)

By W. Burnside. Communicated and received December 13th, 1900.

In the present paper I have extended the method used in the paper "On Groups of Degree n and Class $n-1$," communicated to the Society at the June meeting, so as to make it applicable to any transitive substitution group. As the title of the paper indicates, the method is considered mainly in its application to groups of odd order; but the method itself and the general results of §§ 2 and 4 hold good whether the order is even or odd.

---

* [A remark by a referee leads me to emphasize the above. Absolute orthogonal invariants of a p-ic are invariants of the p-ic and x^2+y^2, and *vice versa*. It has therefore been hastily supposed elsewhere that the complete irreducible invariant system for a p-ic and quadratic produces exactly the complete (absolute) orthogonal system for the p-ic, when x^2+y^2 is taken for the quadratic. A first case of the redundancy of the former system for the latter purpose is exhibited above. The search for complete absolute orthogonal systems is not identical with the search for invariant systems of forms one of which is a quadratic.]

It has been known for some time that a group of order $2n$ (n odd) has a self-conjugate sub-group of order n. This is shown by noticing that when the group is represented as a regular substitution group in $2n$ symbols all its odd operations, and none of its even operations, belong to the alternating group. It is clear that no analogous method of treatment could be used to demonstrate a similar property for a group of order pn, where every prime factor of n is greater than the odd prime p. At the same time, the probability that such a group has an analogous property forces itself on the attention; and it is here shown that this expectation is well founded. The main result arrived at is to show that if p, an odd prime, is the smallest factor of the order of a group, the group must have a self-conjugate sub-group of index p, unless either p^4 or p^3q, where q is a prime factor of p^2+p+1, is a factor of the order.

It is also shown that no odd number less than 40,000 can be the order of a simple group.

1. Let G be a group of order n, and suppose that G is represented as a regular substitution group in the n symbols

$$x_1, x_2, \ldots, x_n.$$

If H is any sub-group of G, whose order is μ ($n = \mu\nu$), the n x's will be interchanged regularly in ν sets of μ each by the operations of H. Let

$$x_1, x_2, \ldots, x_\mu$$

be one of these sets. Then y_1 or

$$x_1+x_2+\ldots+x_\mu$$

is a linear function of the x's which is invariant for each of the operations of H and for no other operations of G. It therefore takes ν distinct values for all the operations of G. Let these be

$$y_1, y_2, \ldots, y_\nu.$$

Each y is the sum of μ x's, and no x occurs in two different y's. The y's therefore are permuted among themselves by the operations of G; and G can be represented as (*i.e.*, is simply or multiply isomorphic with) a permutation group of the y's. The group in the x's is simply or multiply isomorphic with the group in the y's, according as H does not or does contain a self-conjugate sub-group of G. The group of the y's will be represented by the scheme

$$y'_i = y^{(k)}_{i'}$$
$$(i,\ i' = 1, 2, \dots, \nu),$$
$$(k = 1, 2, \dots, n),$$

and will be called G'. If G is multiply isomorphic with G', then, for some two or more values of the affix k,

$$y^{(k)}_{i'} = y_i$$

for each i. In any case, for each affix k the ν symbols

$$y^{(k)}_1,\ y^{(k)}_2,\ \dots,\ y^{(k)}_\nu$$

are the y's in some altered sequence.

The preceding statement is only a slightly modified form of Dyck's procedure* for representing G as a non-regular substitution group.

Suppose now that H is simply or multiply isomorphic with a cyclical group. The necessary and sufficient condition for this is that H shall not be the same as its derived group. If k is the order of a cyclical group with which H is isomorphic, it must be possible to divide the set of symbols

$$x_1,\ x_2,\ \dots,\ x_\mu$$

which are regularly permuted by H into k sets of l each ($\mu = kl$),

$$\begin{array}{llll} x_1, & x_2, & \dots, & x_l, \\ x_{l+1}, & x_{l+2}, & \dots, & x_{2l}, \\ \dots & \dots & & \dots \\ x_{(k-1)l+1}, & x_{(k-1)l+2}, & \dots, & x_{kl}, \end{array}$$

which are cyclically permuted among themselves in the order written by every operation of H. Moreover, if ω is a k-th root of unity, the linear function η_1 or

$$x_1 + \dots + x_l + \omega\,(x_{l+1} + \dots + x_{2l}) + \dots + \omega^{k-1}\,(x_{(k-1)l+1} + \dots + x_{kl})$$

is a relative invariant for every operation of H; any operation of H changing it into $\omega'\eta_1$, where ω' is a power of ω. Hence η_1^k is an absolute invariant of H, and it therefore takes just ν distinct values for all the operations of G. Let

$$\eta_1^k,\ \eta_2^k,\ \dots,\ \eta_\nu^k$$

be these ν values, Each is the k-th power of a linear function of the x's, and no x occurs in two η's. Moreover, if their sequence is suitably chosen, the x's which occur in η_i are the same as those which occur in y_i. Hence the ν k-th powers are permuted among themselves by every operation of G in exactly the same way as the y's.

---

* *Math. Ann.*, Vol. xxii., pp. 90–92.

Now, if any operation of G changes η_i^k into η_j^k, it must change η_i into $\omega'\eta_j$, where ω' is some power of ω. Hence G may be represented as a group of linear substitutions of the η's; and the scheme giving G when so represented will be

$$\eta'_i = \omega_{ki}\eta^{(k)}_{i'}$$
$$(i, i' = 1, 2, \ldots, \nu),$$
$$(k = 1, 2, \ldots, n),$$

where every symbol ω_{ki} represents a power of ω. This group will be called G''. If every ω_{ki} is replaced by unity, the group becomes identical with G', η_i being written everywhere for y_i. If G is simply isomorphic with G', so also is G''. If G is multiply isomorphic with G', G'' may also be so. This will, in fact, be the case if for an operation in which

$$\eta^{(k)}_{i'} = \eta_i \quad (i = 1, 2, \ldots, \nu)$$

the symbols ω_{ki} are not all unity.

Any operation of G'' replaces $\prod_1^\nu \eta_i$ by $\prod_{i=1}^{i=\nu} \omega_{ki} \prod_1^\nu \eta_i$. Hence, unless $\prod_{i=1}^{i=\nu} \omega_{ki}$ is unity for every operation of G'', then G'', and therefore also G, is isomorphic with a cyclical group.

The ν k-th roots of unity, $\omega_{k1}, \omega_{k2}, \ldots, \omega_{k\nu}$, that occur in the specification of any operation of G'' will be called the *factors* of that operation; so that the totality of the operations of G'' for which the products of the factors are unity constitute a self-conjugate sub-group, which contains the derived group.

2. Let p^α be the highest power of a prime p that divides n, the order of G, and let H be a sub-group of order p^α of G. Let I be the greatest sub-group that contains H self-conjugately; and suppose that every operation of I is permutable with every operation of H, so that H must be Abelian. Let S be an operation of H of order p^β, such that there is no operation S' of H for which the relation $S = S'^p$ holds. Then H is isomorphic with a cyclical group of order p^β, and a relative linear invariant η_1 for H may be chosen, such that it is changed by S into $\omega\eta_1$, where ω is a primitive p^β-th root of unity; while it remains unaltered by every operation of that sub-group of H in respect of which H is isomorphic with $\{S\}$.

If S occurs in $1+kp$ sub-groups of order p^α, and if in G' each sub-group of order p^α leaves h symbols unchanged, then the operation of G' which corresponds to S will leave $(1+kp)h$ symbols unchanged. These symbols must be interchanged transitively by the greatest sub-group K in which S is self-conjugate. In fact, the h symbols unchanged by H are interchanged transitively by I, which is contained in K; and K contains operations transforming H into every other sub-group of order p^α in which S enters.

In G'', then, there are $(1+kp)h$ η's which are changed into multiples of themselves by S, and these η's are transformed among themselves with factors by K.

Suppose, if possible, that

$$\eta_1' = \omega\eta_1,\ \eta_2' = \omega^a\eta_2,\ \dots \quad (a \neq 1)$$

represents the effect of S on the η's which are changed into multiples of themselves. K must contain an operation Σ of the form

$$\eta_1' = \omega^b\eta_2,\ \dots,$$

and $\Sigma^{-1}S\Sigma$ would be $\dots,\ \eta_2' = \omega\eta_2,\ \dots .$

This is impossible, since $\Sigma^{-1}S\Sigma = S$. Hence each factor, for the η's which are changed into multiples of themselves by S, must be ω; and, since h is not a multiple of p, their product is a primitive p^β-th root of unity. Suppose next that

$$(y_{s+1}y_{s+2}\cdots y_{s+p^b}) \quad (b \leqslant \beta)$$

is any cycle of the operation that corresponds to S in G'. The corresponding part of S in G'' is

$$\eta_{s+1}' = \omega_1\eta_{s+2},$$

$$\eta_{s+2}' = \omega_2\eta_{s+3},$$

$$\dots \quad \dots \quad \dots$$

$$\eta_{s+p^b} = \omega_{p^b}\eta_{s+1}.$$

Since the p^β-th power of this is identity,

$$(\omega_1\omega_2 \dots \omega_{pb})^{p^{\beta-b}} = 1.$$

The product $\omega_1\omega_2 \dots \omega_{p^b}$ cannot therefore be a primitive p^β-th root of unity; and a similar result holds for each cycle of S in G'.

The product of the factors of S is therefore a primitive p^β-th root of unity, multiplied by $p^{\beta-1}$-th roots; *i.e.*, a primitive p^β-th root of unity. Hence G'', and therefore also G, has a self-conjugate sub-group of index p^β in which neither S nor any of its powers occurs. The same reasoning may be repeated with this self-conjugate sub-group, leading at last to the result that G has a self-conjugate sub-group of index p^α.

From this general result the following particular ones are at once deduced. If p is the smallest prime, and p^α the highest power of p, which divide the order of a group G, and if the sub-groups of order p^α are Abelian groups with either one or two generating operations, then G has a self-conjugate group of index p^α. The case $p = 2$, and 3 a factor of the order, is a possible exception.

In fact, when these conditions are satisfied, the order of the group of isomorphisms* of a sub-group of order p^α is not divisible by any prime greater than p, and therefore every operation of I (in the original statement) is necessarily permutable with every operation of H.

In particular, if G is a group of odd order $p^\alpha m$ ($\alpha = 1$ or 2), where p is less than any prime factor of m, then G has a self-conjugate sub-group of order m.

For in this case all the conditions are necessarily satisfied.

If G is a group of odd order p^3m, where p is less than any prime factor of m, and if the sub-groups of order p^3 are Abelian, while m and p^2+p+1 contain no common factor, then G has a self-conjugate sub-group of order m.

For the only isomorphisms of order greater than p, which an Abelian group of order p^3 can admit, have factors of p^2+p+1 for their order.

Also, if the odd order of G contains an unrepeated prime factor q, of the form 2^n+1, then G has a self-conjugate sub-group of index q.

Another special result of the general theorem is the following, which applies alike to groups of odd and of even order:—

If p^α is the highest power of a prime p which divides the order $p^\alpha m$ of a group G, and if every operation of a sub-group of G of order p^α is a self-conjugate operation of G, then G is the direct product of groups of orders p^α and m.

For in this case G has self-conjugate sub-groups of orders m and p^α.

3. Before proceeding to a second application of the general method of § 1, it will be necessary to prove a property of certain groups whose order is a power of a prime, when represented as substitution groups affected with "factors." I consider, first, the case in which the substitution group is a cyclical group in p symbols generated by $(x_1 x_2 \ldots x_p)$, while the factors are p-th roots of unity. The general

---

* *Theory of Groups*, p. 251.

operation of such a group will be

$$x_1' = \omega_1 x_{1+k},$$

$$x_2' = \omega_2 x_{2+k},$$

$$\dots \quad \dots \quad \dots$$

$$x_p' = \omega_p x_{p+k},$$

where $\omega_1, \omega_2, \dots, \omega_p$ are p-th roots, and the suffixes of the x's are reduced mod. p. The total number of such operations, *i.e.*, the order of the most general group of the kind, is clearly p^{p+1}; and the order of the self-conjugate sub-group in which each symbol is merely multiplied by a factor is p^p. Suppose, now, that such a group contains an operation S,

$$x_r' = \omega^{a_r} x_r \quad (r = 1, 2, \dots, p),$$

for which the product of the factors is not unity, so that

$$a_1 + a_2 + \dots + a_p \not\equiv 0 \mod p.$$

The group then contains the p operations

$$x_r' = \omega^{a_{r+k}} x_r \quad (r = 1, \dots, p),$$

$$(k = 0, 1, \dots, p-1),$$

obtained by transforming S by the powers of $(x_1 x_2 \dots x_p)$; and therefore also the operation

$$x_r' = \omega^{\sum_k y_k a_{r+k}} x_r \quad (r = 1, 2, \dots, p).$$

where $y, y_1, \dots, y_{p-1}$ are any integers. Consider now the system of congruences

$$\sum_k y_k a_{r+k} = z_r \quad (r = 1, 2, \dots, p).$$

The determinant of the left-hand side

$$\begin{vmatrix} a_1 & a_2 & \dots & a_p \\ a_p & a_1 & \dots & a_{p-1} \\ \dots & & \dots & \dots \\ a_2 & a_3 & \dots & a_1 \end{vmatrix}$$

is easily shown to be congruent to $a_1 + a_2 + \dots + a_p$; and, since by supposition this is not zero, mod. p, the system of congruences have a solution in integers for the y's, whatever integers the z's may be. The group therefore contains the p operations

$$x_s' = x_s \quad (s \neq r), \quad x_r' = \omega x_r.$$

But these generate a sub-group of order p^p; and, combining this with

$(x_1 x_2 \dots x_p)$, the order of the group is p^{p+1}. Hence, if the order of a group of the kind considered is less than p^{p+1}, the product of the factors must be unity for every operation which changes each symbol into a multiple of itself. It is to be noticed that no inference can be drawn with respect to the operations which interchange the symbols cyclically.*

Still supposing that the factors are p-th roots of unity, I consider now the case where the substitution group is a transitive group of degree p^α. Let T be any self-conjugate operation of order p of the substitution group. The symbols left unchanged by any operation S of the substitution group are permuted in sets of p by T. If $x_1, x_2, \dots, x_p$ is such a set of symbols, then, in the group as affected by factors, each is replaced by a multiple of itself by the operation S. If the product of the p factors affecting these symbols were not unity, then T and S would, as regards these p symbols, generate a group of order p^{p+1} by the preceding result. Hence, again in this case, if the order of the group is less than p^{p+1}, the product of the factors of the unchanged symbols of any operation must be unity. Now, for an operation of order p, the product of the factors for a set of p symbols which are permuted cyclically by the operation is necessarily unity. In fact, let

$$x_1' = \omega_1 x_2,\quad x_2' = \omega_2 x_3,\quad \dots,\quad x_p' = \omega_p x_1$$

be the operation, so far as it affects the symbols in question. The p-th power of this substitution is

$$x_r' = \omega_1 \omega_2 \dots \omega_p x_r \quad (r = 1, 2, \dots, p);$$

and, since this must be identity, the product of the factors is unity, as stated.

The general result of this discussion may then be stated thus:—If a group of order p^α $(\alpha \leqslant p)$ be represented as a transitive substitution group affected by factors which are p-th roots of unity, the product of the factors for any operation of order p belonging to the group is unity.

4. Returning now to the general theorem, let p^α, as before, be the highest power of a prime p which divides the order $p^\alpha m$ of a group G. Let H be a sub-group of order p^α, and let I be the greatest sub-group

---

* In fact, $x_1' = \omega x_2,\quad x_2' = x_3,\quad \dots,\quad x_p' = x_1$

and $x_1' = x_1,\quad x_2' = \omega x_2,\quad \dots,\quad x_p' = \omega^{p-1} x_p$

generate a group of order p^3 in which ω is the product of the factors for one of the cyclical operations.

that contains H self-conjugately. Suppose also that every operation of I, whose order is relatively prime to p, is permutable with every operation of H. Let η_1 be a relative invariant for H, which is unaltered by every operation of a self-conjugate sub-group of index p of H, and is changed into $\omega\eta_1$ by some operation S of H not occurring in this sub-group.

If in G' the sub-group H leaves μ symbols unchanged, they must be transitively permuted by the operations of I. In G'' each of these symbols is changed into a multiple of itself by every operation of H. Moreover, S changes η_1 into $\omega\eta_1$; and therefore each of the other $\mu-1$ must be changed by S into ω times itself, as otherwise S could not be permutable with every operation of I whose order is relatively prime to p. The remaining $m-\mu$ symbols are permuted transitively in sets of p^a, p^b, ... by the operations of H in G'. Hence, by the result obtained above, if the order of S is p, and if $a \leqslant p$, the product of the factors of S, so far as these $m-\mu$ symbols are concerned, is unity. Under these conditions, then, the product of all the factors of S is ω^μ, and μ is necessarily relatively prime to p. Hence G'', and therefore also G, has a self-conjugate sub-group of index p.

If p (>2) is the smallest prime which divides the order of G, and if $\alpha = 3$, while the sub-groups of order p^3 are not Abelian, all the conditions imposed are satisfied. In fact, the primes dividing the order of the group of isomorphisms of H must be factors of $(p-1)(p^2-1)$; while the only two types of non-Abelian groups of order p^3 both contain operations of order p which do not enter in a suitably chosen sub-group of order p^2. Hence:—

If p is the smallest prime dividing the order of a group G of odd order, and if p^3 is the highest power of p which divides the order, then, if the sub-groups of order p^3 are not Abelian, the group has a self-conjugate sub-group of index p^3.

Combining this with the previous result, it follows that, if $p\,(>2)$ be the smallest prime and p^α the highest power of p which divide the order of a group, then the group must have a self-conjugate sub-group of index p^α, unless (i) $\alpha \geqslant 4$ or (ii) $\alpha = 3$, and a factor of p^2+p+1 divides the order.

5. From the preceding results it is not difficult to show that no odd number which is the product of six primes can be the order of a simple group.

If p_1, p_2, p_3, ... denote odd primes in ascending order of magnitude, it follows from the preceding theorems and from the results contained in chap. xv. of my book on the *Theory of Groups* (especially Theorem IV.) that, (i) $p_1^4 p_2 p_3$, (ii) $p_1^3 p_2^3$, (iii) $p_1^3 p_2^2 p_3$, (iv) $p_1^3 p_2 p_3^2$, (v) $p_1^3 p_2 p_3 p_4$ are the only possible forms for the order of such a group. Moreover, in the last four, a sub-group of order p_1^3 must be Abelian with no operations of order p_1^2; and one of the primes p_2, p_3, p_4 must be a factor of $p_1^2+p_1+1$.

(i) *Order* $p_1^4 p_2 p_3$.—There must be $p_2 p_3$ sub-groups of order p_1^4; otherwise the group can be represented as of prime degree and is certainly soluble (*Proc. Lond. Math. Soc.*, Vol. XXXIII., p. 177). If the operations of these sub-groups were all distinct, there would be a self-conjugate sub-group of order $p_2 p_3$. If some, or all, of the self-conjugate operations of a sub-group of order p_1^4 occur in no other sub-group of order p_1^4, every operation common to two sub-groups of order p_1^4 must be permutable with an operation of order p_2 or p_3. In this case there would be exactly $p_2 p_3 - 1$ operations whose orders are divisible by p_2 or p_3, and the group would be composite. If any operation were self-conjugate in more than one sub-group of order p_1^4, it would be one of p_2 or p_3 conjugate operations, and again the group would be composite. Lastly, if an operation P of order p_1 is self-conjugate in one sub-group of order p_1^4, and enters in another as one of p_1 or more conjugate operations, there must be[*] an operation Q (of order p_2 or p_3) such that P, $Q^{-1}PQ$, $Q^{-2}PQ^2$, ... are permutable with each other. These would generate a sub-group of order p_1^3, which would be common to several sub-groups of order p_1^4, and would therefore be one of p_3 or p_2 conjugate sub-groups. The group again therefore would be composite.

(ii) *Order* $p_1^3 p_2^3$.—If there are p_1^3 sub-groups of order p_2^3, they must, if the group be simple, have common operations; and, since p_1^3 is the only factor of the order which is congruent to unity, mod. p_2, the totality of these common operations form a self-conjugate sub-group. The group is therefore composite.

(iii) and (iv) *Order* $p_1^3 p_\beta^2 p_\gamma$.—If an operation of order p_1 is permutable with one of order p_β, there must be a sub-group of order $p_1^3 p_\beta$, and this must contain a sub-group of order p_β self-conjugately. This sub-group would be one of p_γ conjugate sub-groups, and the group would therefore be composite. It may be assumed therefore that there are no operations of order $p_1 p_\beta$.

---

[*] *Theory of Groups*, p. 100.

If an operation of order p_γ is conjugate with one of its own powers, then $p_1^2 p_\beta^2 (p_\gamma - 1)$ is the greatest number of operations the group can contain whose orders are divisible by p_γ. If a sub-group of order p_β^2 is contained self-conjugately in a greater sub-group, then $p_1^2 p_\gamma (p_\beta^2 - 1)$ is the greatest number of operations, whose orders are powers of p_β, that can be contained in the group. Lastly, $p_\beta p_\gamma (p_1^3 - 1)$ or $p_\beta^2 (p_1^3 - 1)$ is the greatest number of operations of order p_1 the group can contain. Now the sum of these numbers is less than $\frac{2}{p_1} + \frac{1}{p_\beta}$ times the order of the group; and, since $\frac{2}{p_1} + \frac{1}{p_\beta}$ is necessarily less than unity, this is impossible. Hence either an operation of order p_γ is not conjugate with any of its powers or a sub-group of order p_β^3 is contained self-conjugately in no greater sub-group. In either case the group is composite, from the results of § 2.

(v) *Order* $p_1^3 p_2 p_3 p_4$. — Unless operations of each of the orders p_2, p_3, p_4 are conjugate to powers of themselves, the group is certainly composite, by § 2. If the condition is satisfied, the greatest possible numbers of operations contained in the group whose orders are divisible by p_2, p_3, and p_4 respectively are

$$p_1^2 p_3 p_4 (p_2 - 1), \quad p_1^2 p_2 p_4 (p_3 - 1), \quad p_1^2 p_2 p_3 (p_4 - 1).$$

The greatest possible number of operations of order p_1 is $p_3 p_4 (p_1^3 - 1)$. The sum of unity with these four numbers must be equal to or greater than the order of the group. This sum is, however, less than $\frac{3}{p_1} + \frac{1}{p_2}$ times the order. Hence, unless p_1 is 3, the group is certainly composite.*

If p_1 is 3, the group is composite unless one of the other prime factors is 13. The order must therefore be $3^3 . 13 . pq$: and the group has a sub-group of order $3^3 . 13$, in which there are just 13 sub-groups of order 3 all conjugate to each other.

---

* [*Note, January 19th*, 1901.—This method, combined with the results of § 2, may be used to prove in a somewhat similar way that a group of order $p_1^{\alpha_1} p_2^{\alpha_2} .. p_n^{\alpha_n}$, where each of the indices $\alpha_2, \alpha_3, \ldots, \alpha_n$ is either 1 or 2, and where $p_1 > n - 1$, is composite, with a possible exception in the case where there are $p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_n^{\alpha_n}$ sub-groups of order $p_1^{\alpha_1}$.]

The discussion of this particular case presents no serious difficulty. It may be shown at once that the group is composite if it contains operations of composite order; and that the only constitution of the group, which is consistent with its being simple, is one in which there are

$3^2 . 13p$ sub-groups of order q,
$3^2 . 13q$,, ,, p,
$3^2 . p . q$,, ,, 13,
and pq ,, ,, 3^3,

without common operations. This leads to the equation

$$17pq-117(p+q)+1=0;$$

and 7 and 409 is the only pair of primes satisfying this equation. The group would then contain $1+2 . 409$ sub-groups of order 409; and it could be represented as a primitive group of degree $1+2 . 409$, in which the sub-groups that leave one symbol unchanged permute the remaining ones in two equal transitive sets. The group would also contain operations of order 13 which permute all the symbols. That such a group is non-existent is shown on p. 179 of my paper, "On Some Properties of Groups of Odd Order" (*Proc. Lond. Math. Soc.*, Vol. XXXIII., pp. 162–185).

6. The number of prime factors in the order of a simple group of odd order is thus shown to be not less than 7. Combining this with the limitations on the order involved by the results of § 2, it will be found that the only odd numbers less than 40,000 which can possibly be the order of such a group are:—$3^5.7.13$, $3^5.7.19$, $3^4.5^3$, $3^4.5^2.7$, $3^4.5^2.11$, $3^4.5^2.13$, $3^4.5^2.19$. There is no difficulty in verifying that no one of these numbers can be the order of a simple group; so that 40,000 is a lower limit for the order, if odd, of a simple group. There is no doubt that by a similar detailed examination this limit might be carried a good deal further; but, in view of the possibility of some more general properties of groups of odd order being discovered, it seems hardly worth while to carry a mere method of enumeration beyond the point reached.

On Discriminants and Envelopes of Surfaces.

By R. W. H. T. Hudson.

Received November 27th, 1900. Communicated December 13th, 1900.

1. Functions of several arguments frequently occur in analysis as discriminants of binary forms in which the arguments figure as coefficients. Examples occur in the theory of envelopes of curves and surfaces involving one parameter, and in the theory of singular solutions of ordinary differential equations. It is proposed in the following short paper, first, to obtain in a general manner certain properties of the discriminant of a binary form (or polynomial), and then to apply the results to the case of a family of algebraic surfaces.

Let F be a polynomial in t, and let dashes indicate differentiation with respect to t; then the discriminant Δ of F is the resultant of F and F', and can be expressed in the form

$$\Delta \equiv AF+BF'$$

where A and B are also polynomials in t.*

The advantage of this expression for Δ lies in the fact that all the arguments appearing explicitly in the dexter are independent, and, further, that t may have an arbitrary value, since it does not occur in Δ.

Now, when the relation among the coefficients expressed by $\Delta = 0$ is satisfied, the equations $F=0$, $F'=0$ have a common root, say t_1. In the following investigation the symbol " $=$ " is used when equality holds under the conditions $\Delta = 0$, $t = t_1$; while the symbol " $\equiv$ " is used when equality holds for all values of the coefficients and t.

2. In order to find the values of A, B, A', B', ..., when $\Delta = 0$ and $t = t_1$, we make use of the fact that Δ is independent of t. Then, by differentiation,

$$\begin{aligned} \Delta &\equiv AF+BF', \\ 0 \equiv \Delta' &\equiv A'F+(A+B')F'+BF'', \\ 0 \equiv \Delta'' &\equiv A''F+(2A'+B'')F'+(A+2B')F''+BF'''. \end{aligned}$$

---

* Burnside and Panton, *Theory of Equations*, 1892, p. 360.

Putting $\Delta = 0$, $t = t_1$ in these identities, we obtain

$$B = 0,$$

$$A + 2B' = 0.$$

3. Let δ denote any differentiating operator affecting only the coefficients in F, and not affecting t. Then

$$\delta\Delta \equiv \delta A . F + A . \delta F + \delta B . F' + B . \delta F';$$

therefore $\delta\Delta = A\delta F$.*

Further, if we calculate $\delta_1\delta_2\Delta$, and use the above relations, together with $\delta\Delta' \equiv 0$, we easily obtain

$$F''\delta_1\delta_2\Delta = A\,\{F''\delta_1\delta_2 F - \delta_1 F'\delta_2 F'\} + \delta_1 F\,\{F''\delta_2 A - A'\delta_2 F'\}$$
$$+ \delta_2 F\{F''\delta_1 A - A'\delta_1 F'\}$$

and, making $\delta_1 \equiv \delta_2$,

$$F''\delta^2\Delta = A\,\{F''\delta^2 F - (\delta F')^2\} + 2\delta F\{F''\delta A - A'\delta F'\}.$$

Thus we obtain derivatives of Δ in terms of those of F and A.

4. Next suppose that the common root of $F = 0$ and $F' = 0$ is a triple root of $F = 0$. Then we have

$$F'' = 0.$$

In this case the identity $\Delta' \equiv 0$ gives no relation among A, B, ... It is easy to verify that

$\Delta'' \equiv 0$ gives $B = 0$,

$\Delta''' \equiv 0$ gives $A + 3B' = 0$,

$\delta\Delta' \equiv 0$ gives $A'\delta F + (A + B')\delta F' = 0$.

---

* More generally, if Δ is the resultant of F and G, and $\Delta \equiv AF + BG$, then

$$\delta\Delta = A\delta F + B\delta G.$$

Let $F \equiv a_0 + a_1 t + \ldots + a_n t^n$,

and put $\delta \equiv \dfrac{\partial}{\partial a_r}$;

therefore $\dfrac{\partial\Delta}{\partial a_r} = A\dfrac{\partial F}{\partial a_r} = At_1^r$;

whence the known result $\dfrac{\partial\Delta}{\partial a_r} : \dfrac{\partial\Delta}{\partial a_s} = t_1^r : t_1^s$.

See Burnside and Panton, *Theory of Equations*, 1892, p. 360.

This equation cannot be true for all forms of δ unless [*]

$$A' = 0,$$

$$A + B' = 0;$$

therefore $$A = 0, \quad B' = 0.$$

Then $$\Delta^{\text{iv}} \equiv 0 \quad \text{gives} \quad 4A' + 6B'' = 0;$$

therefore $$B'' = 0.$$

$$\Delta^{\text{v}} \equiv 0 \quad \text{gives} \quad A'' + B''' = 0.$$

Thus, when $\Delta = 0$, $F = 0$, $F' = 0$, $F'' = 0$, we have

$$A = 0, \quad A' = 0,$$

$$B = 0, \quad B' = 0, \quad B'' = 0,$$

$$A'' + B''' = 0.$$

5. From these relations follow

$$\delta\Delta = 0,$$

$$\delta_1\delta_2\Delta = \delta_1 A \,.\, \delta_2 F + \delta_2 A \,.\, \delta_1 F + \delta_1 B \,.\, \delta_2 F' + \delta_2 B \,.\, \delta_1 F';$$

but $$\delta\Delta'' \equiv 0 = A''\delta F + \delta B \,.\, F''';$$

therefore $$\delta_1\delta_2\Delta = \delta_1 F\{F'''\delta_2 A - A''\delta_2 F'\} + \delta_2 F\{F''\delta_1 A - A''\delta_1 F'\}.$$

We proceed to show that $F'''\delta A - A''\delta F'$ contains δF as a factor; so that $\delta_1\delta_2\Delta$ is equal to $\delta_1 F \,.\, \delta_2 F$ multiplied by a factor which does not involve δ. This factor is not important; so it is sufficient to prove that when δF vanishes $F'''\delta A - A''\delta F'$ vanishes also.

Suppose, then, that $\delta F = 0$.

We have

$0 \equiv \delta\Delta''$; therefore $\delta B = 0$.

$0 \equiv \delta\Delta'''$; therefore $(\delta A + 3\delta B')F''' + (3A'' + B''')\delta F' = 0$.

$0 \equiv \Delta^{V}$; therefore $A'' + B''' = 0$.

$0 \equiv \delta^2\Delta'$; therefore $\delta A + \delta B' = 0$;

therefore $F'''\delta A - A''\delta F' = 0$.

Thus, under the conditions $\Delta = 0$, $t =$ triple root of $F = 0$, we have

$$\delta\Delta = 0,$$

$$\delta_1\delta_2\Delta = M \,.\, \delta F_1\, \delta_2 \,.\, F,$$

$$\delta^2\Delta = M(\delta F)^2.\text{[†]}$$

---

[*] *E.g.*, putting $\delta \equiv \frac{\partial}{\partial a_r}$, we must have $A' t_1^r + (A + B') r t_1^{r-1} = 0$ for $r = 1, \ldots, n$.

[†] Some of the preceding results were given in 1868 by Prof. Henrici (*Proc. Lond. Math. Soc.*, Vol. II., p. 104). See also Vol. XIX., p. 566 (1888), where Prof. Hill finds expressions for $\delta_1\delta_2\Delta$ and $\delta^2\Delta$.

6. To apply the preceding analysis to the theory of envelopes of surfaces, we suppose that F is algebraic in coordinates x, y, z, as well as in the parameter t. Then the equation

$$F(xyzt) = 0 \tag{1}$$

represents a family of surfaces one member of which corresponds to each value of t.

The surface t cuts the surface $t+dt$ in the curve

$$\left.\begin{array}{r} F=0 \\ \dfrac{\partial F}{\partial t}=0 \end{array}\right\}. \tag{2}$$

The locus of this curve, as t varies, is the surface Δ, which has the form

$$\Delta \equiv AF+BF_t = 0. \tag{3}$$

We infer from § 2 that the surface $B(xyzt) = 0$ passes through the curve (2).

Hence, from (3), Δ *touches* F all along (2); so that the name *envelope* is justified. This fact is expressed also by the equation

$$\delta\Delta = A\delta F$$

when we put $\delta \equiv (X-x)\dfrac{\partial}{\partial x}+(Y-y)\dfrac{\partial}{\partial y}+(Z-z)\dfrac{\partial}{\partial z}$.

7. The characteristic (2) meets a consecutive one where

$$F=0,\quad F_t=0,\quad F_{tt}=0; \tag{4}$$

i.e., in a finite number of points. At any one of these points we have, from § 5, $\dfrac{\partial\Delta}{\partial x}=0,\quad \dfrac{\partial\Delta}{\partial y}=0,\quad \dfrac{\partial\Delta}{\partial z}=0,$

showing that the point is a singular point of the surface Δ. The tangent cone is given by

$$\delta^2\Delta = 0$$

where δ has the form given above. But, from § 5,

$$\delta^2\Delta = M(xyzt)\,(\delta F)^2;$$

so that the tangent cone breaks up into two coincident planes, $\delta F = 0$, which is the tangent plane to the surface F at the point considered.

Hence the locus of the points (4) is a *cuspidal edge* on Δ.

From § 4 we have

$$A = 0 = A_t,$$
$$B = 0 = B_t = B_{tt}.$$

Hence the edge of Δ lies on the envelope of A, and is the same as the edge of the envelope of B.

Further, the equation $A''\delta F + F'''\delta B = 0$ of § 5 shows that the surfaces F and B touch at the points (4). Hence the envelopes of F and B not only have the same curve for edge, but *have the same tangent plane at every point of it.*

8. When certain conditions equivalent to two independent conditions are satisfied, the equations $F = 0$, $F_t = 0$ have two distinct common roots t_1, t_2. In the present interpretation these conditions represent a curve which is the locus of points where (2) meets a non-consecutive characteristic. Applying the results of § 3, we have $\delta\Delta = A\delta F$ for $t = t_1$ and $t = t_2$ and all forms of δ; therefore $A = 0$ for $t = t_1, t_2$; therefore $\delta\Delta = 0$;[*] so that these points are singular points on $\Delta = 0$.

Further, putting $A = 0$,

$$\delta^2\Delta = 2[\delta F]_{(t=t_1)}\left[\delta A - \frac{A'}{F''}\delta F'\right]_{t=t_1}$$

$$= 2[\delta F]_{(t=t_2)}\left[\delta A - \frac{A'}{F''}\delta F'\right]_{t=t_2};$$

so that the tangent cone at one of these points consists of the two planes

$$\delta F(t_1) = 0,$$

$$\delta F(t_2) = 0,$$

which are the tangent planes to the two surfaces F which pass through the point. *The locus of these points is therefore a nodal line on Δ.*

We infer that each characteristic meets a non-consecutive characteristic where it meets the corresponding surface $A = 0$.

Again, from § 2, putting $A = 0$, we find

$$B' = 0.$$

Then, since B and B' vanish for $t = t_1, t_2$, the locus is also a nodal line for the envelope of B.

Again, $\delta\Delta' = 0$ gives

$$A'\delta F + \delta B \,.\, F'' = 0 \quad (t = t_1, t_2);$$

so that the two surfaces B, passing through any point of the nodal line, touch respectively the two surfaces F through the same point—that is, *corresponding sheets of the envelopes of F and B touch along their common nodal line.*

---

[*] See Salmon, *Higher Algebra*, 1885, p. 97.

9. To sum up. The envelope of a surface involving algebraically one parameter is a surface possessing a cuspidal edge and a nodal line. It is possible to find another surface involving one parameter to a degree less high by one (but being itself, in general, of higher degree) such that the envelope of this second surface has the same singular lines as the former envelope and the same tangent planes at all points of these lines.

An Addition Theorem for Hyperelliptic Theta-Functions. By

A. L. DIXON. Received and read December 13th, 1900.

In the following paper relations between the hyperelliptic Θ-functions for three or four arguments whose sum is zero are deduced as a direct integral of the differential equations involved.

The method of integration is an extension of one given by Cayley (*Coll. Works*, Vol. XI., p. 73) as that by which he originally found his well known formula in elliptic functions, viz., when

$$u_1+u_2+u_3+u_4 = 0,$$

$$\kappa^2\kappa'^2\,\Pi_\iota \operatorname{sn} u_\iota - \kappa^2\,\Pi_\iota \operatorname{cn} u_\iota + \Pi_\iota \operatorname{dn} u_\iota = \kappa'^2 \quad (\iota = 1, 2, 3, 4).$$

and has a certain geometrical interest.

The proof is given in full merely for the double Θ-functions, but is at once capable of extension to any order; the necessary modifications for the triple functions are given in § 12.

1. Take
$$\Sigma\,\frac{x_\iota^2}{a_\iota+\lambda} = 1 \quad (\iota = 1, 2, 3, 4, 5) \qquad (1)$$

as the equation of a set of confocal ${}_2R_4$'s* in a space S_5, and let p, q, r, s, t be the values of λ for the five members of the set through any point. Then

$$\Sigma\,\frac{x_\iota^2}{a_\iota+\lambda} - 1 \equiv -\frac{(\lambda-p)(\lambda-q)(\lambda-r)(\lambda-s)(\lambda-t)}{\Pi\,(a_\iota+\lambda)}; \qquad (2)$$

---

* ${}_pR_q$ is used to denote a continuum with q degrees of freedom and of degree p in the coordinates.

and therefore

$$x_\iota^2 = \frac{(a_\iota+p)(a_\iota+q)(a_\iota+r)(a_\iota+s)(a\ +t)}{f'(-a_\iota)}, \tag{3}$$

writing $$f(\lambda) \equiv \Pi\,(a_\iota+\lambda);$$

therefore $$2\frac{dx_\iota}{dp} = \frac{x_\iota}{a_\iota+p}, \tag{4}$$

and, if ds_p be written for an element of distance along the direction for which p alone varies, q, r, s, t being kept constant, we get

$$4ds_p^2 = \Sigma_\iota \frac{x_\iota^2}{(a_\iota+p)^2}\,dp^2 = \frac{(p-q)(p-r)(p-s)(p-t)}{f(p)}\,dp^2. \tag{5}$$

2. Now consider those points (found to lie on four straight lines) which are common to the two surfaces

$$\Sigma\frac{x_\iota^2}{a_\iota+s} = 1,\ (S);\quad \Sigma\frac{x_\iota^2}{a_\iota+t} = 1,\ (T); \tag{6}$$

and also to the tangent ${}_1R_4$'s to S and T at any point h_1, h_2, h_3, h_4, h_5 (say the point h_ι) which is on both: viz.,

$$\Sigma\frac{x_\iota h_\iota}{a_\iota+s} = 1,\ (S');\quad \Sigma\frac{x_\iota h_\iota}{a_\iota+t} = 1,\ (T'). \tag{7}$$

Taking first any one of the system

$$\Sigma\frac{x_\iota^2}{a_\iota+\lambda} = 1,$$

the tangent ${}_2R_4$ from h_ι (in three dimensions this would be the tangent cone) is given by the equation

$$\left(\Sigma\frac{x_\iota^2}{a_\iota+\lambda}-1\right)\left(\Sigma\frac{h_\iota^2}{a_\iota+\lambda}-1\right) = \left(\Sigma\frac{x_\iota h_\iota}{a_\iota+\lambda}-1\right)^2,$$

and this when referred to the normals to the five confocals through h_ι as principal axes will take the form*

$$\frac{\xi_p^2}{p-\lambda}+\frac{\xi_q^2}{q-\lambda}+\frac{\xi_r^2}{r-\lambda}+\frac{\xi_s^2}{s-\lambda}+\frac{\xi_t^2}{t-\lambda} = 0, \tag{8}$$

where p, q, r, s, t are the parameters of the five confocals through h_ι. Putting $\lambda = s$, we get $\xi_s = 0$, and then, putting $\xi_t = 0$, we get, as the intersection of S, S', and T',

---

* *Cf.* Salmon, *Geometry of Three Dimensions*, p. 149, §§ 171–3.

$$\frac{\xi_p^2}{p-s}+\frac{\xi_q^2}{q-s}+\frac{\xi_r^2}{r-s}=0, \quad \xi_s=0, \quad \xi_t=0. \tag{9}$$

Similarly, as the intersection of T, S', and T', we get

$$\frac{\xi_p^2}{p-t}+\frac{\xi_q^2}{q-t}+\frac{\xi_r^2}{r-t}=0, \quad \xi_s=0, \quad \xi_t=0, \tag{10}$$

and therefore, combining these two sets of equations, the common points of S, T, S', T' are given by

$$\xi_s=0, \quad \xi_t=0, \tag{11}$$

$$\frac{\xi_p^2}{(p-s)(p-t)(q-r)}=\frac{\xi_q^2}{(q-s)(q-t)(r-p)}=\frac{\xi_r^2}{(r-s)(r-t)(p-q)},$$

the equations of four lines.

3. Now writing for ξ_p, ds_p, for ξ_q, ds_q, and for ξ_r, ds_r, we get, as the differential equation of the four lines, on substituting from (5),

$$\sqrt{\frac{(p-q)(p-r)}{q-r}}\,\frac{dp}{\sqrt{f(p)}}=\pm\sqrt{\frac{(q-p)(q-r)}{r-p}}\,\frac{dq}{\sqrt{f(q)}}$$
$$=\pm\sqrt{\frac{(r-p)(r-q)}{p-q}}\,\frac{dr}{\sqrt{f(r)}};$$

or, say,
$$\frac{1}{q-r}\,\frac{dp}{\sqrt{P}}=\frac{\epsilon}{r-p}\,\frac{dq}{\sqrt{Q}}=\frac{\epsilon'}{p-q}\,\frac{dr}{\sqrt{R}} \quad (\epsilon^2=\epsilon'^2=1); \tag{12}$$

or, finally,
$$\left.\begin{aligned}\frac{dp}{\sqrt{P}}+\epsilon\frac{dq}{\sqrt{Q}}+\epsilon'\frac{dr}{\sqrt{R}}&=0\\ \frac{p\,dp}{\sqrt{P}}+\epsilon\frac{q\,dq}{\sqrt{Q}}+\epsilon'\frac{r\,dr}{\sqrt{R}}&=0\end{aligned}\right\}, \tag{13}$$

where $P\equiv f(p)$, &c., &c.

4. Thus the equations S, T, S', T' give an algebraical integral of these two equations (13), which are equivalent to

$$\left.\begin{aligned}\int\frac{dp}{\sqrt{P}}-\int\frac{dp_0}{\sqrt{P_0}}+\epsilon\left(\int\frac{dq}{\sqrt{Q}}-\int\frac{dq_0}{\sqrt{Q_0}}\right)+\epsilon'\left(\int\frac{dr}{\sqrt{R}}-\int\frac{dr_0}{\sqrt{R_0}}\right)&=0\\ \int\frac{p\,dp}{\sqrt{P}}-\int\frac{p_0\,dp_0}{\sqrt{P_0}}+\epsilon\left(\int\frac{q\,dq}{\sqrt{Q}}-\int\frac{q_0\,dq_0}{\sqrt{Q_0}}\right)+\epsilon'\left(\int\frac{r\,dr}{\sqrt{R}}-\int\frac{r_0\,dr_0}{\sqrt{R_0}}\right)&=0\end{aligned}\right\}, \tag{14}$$

where p_0, q_0, r_0, s, t are the parameters for the point h_ι. Expressing the x in terms of p, q, r, s, t, and the h in terms of p_0, q_0, r_0, s, t, we get

$$\frac{\Sigma_\iota\,(a_\iota+t)\sqrt{a_\iota+p\,.\,a_\iota+p_0\,.\,a_\iota+q\,.\,a_\iota+q_0\,.\,a_\iota+r\,.\,a_\iota+r_0}}{f'(-a_\iota)}=1,$$

$$\frac{\Sigma_\iota\,(a_\iota+s)\sqrt{a_\iota+p\,.\,a_\iota+p_0\,.\,a_\iota+q\,.\,a_\iota+q_0\,.\,a_\iota+r\,.\,a_\iota+r_0}}{f'(-a_\iota)}=1,$$

or we may put

$$\frac{\Sigma_\iota\,(a_\iota+\lambda)\sqrt{a_\iota+p\,.\,a_\iota+p_0\,.\,a_\iota+q\,.\,a_\iota+q_0\,.\,a_\iota+r\,.\,a_\iota+r_0}}{f'(-a_\iota)}=1, \qquad (15)$$

where λ has any value we please.

5. For convenience I rewrite this result in the form it assumes when the function under the square root (*e.g.*, P) is by a linear transformation changed from a product of five factors to a product of six, and further I change the notation.

Putting $f(x)=X=a-x\,.\,b-x\,.\,c-x\,.\,d-x\,.\,e-x\,.\,f-x,$

and writing (Cayley, *Coll. Works*, Vol. x., p. 564)

$$\sigma u+\tau v=\int_x^\infty\frac{dx}{\sqrt{X}}-\int_y^\infty\frac{dy}{\sqrt{Y}},$$

$$\varpi u+\rho v=\int_x^\infty\frac{x\,dx}{\sqrt{X}}-\int_y^\infty\frac{y\,dy}{\sqrt{Y}},$$

where σ, τ, ϖ, ρ are constants, I replace (14) by

$$\left.\begin{aligned}\Sigma_\iota\left(\int\frac{dx_\iota}{\sqrt{X_\iota}}-\int\frac{dy_\iota}{\sqrt{Y_\iota}}\right)&=0\\ \Sigma_\iota\left(\int\frac{x_\iota\,dx}{\sqrt{X_\iota}}-\int\frac{y\,dy}{\sqrt{Y_\iota}}\right)&=0\end{aligned}\right\}\ (\iota=1,2,3), \qquad (16)$$

or by $$u_1+u_2+u_3=0, \quad v_1+v_2+v_3=0;$$

then (15) becomes

$$\Sigma_s\,(s-\lambda)\,\frac{\Pi_\iota\sqrt{s-x_\iota\,.\,s-y_\iota}}{f'(s)}=0$$

$$(s=a,b,c,d,e,f;\ \iota=1,2,3). \qquad (17)$$

6. In consideration of this result as a relation among double theta-functions I adopt Cayley's single and double letter notation (*Coll. Works*, Vol. x., pp. 501, 502, and 190).

This notation is, the equations denoting merely proportion,

$$A = \alpha\sqrt{\overline{a-x}\,.\,\overline{a-y}}, \quad B = \beta\sqrt{\overline{b-x}\,.\,\overline{b-y}}, \ \dots \text{ (six odd functions)},$$

$$(AB) = (ABF\,.\,CDE)$$

$$= \frac{(\alpha\beta)}{x-y}\left\{\sqrt{\frac{\overline{a-x}\,.\,\overline{b-x}\,.\,\overline{f-x}}{\overline{c-y}\,.\,\overline{d-y}\,.\,\overline{e-y}}} + \sqrt{\frac{\overline{a-y}\,.\,\overline{b-y}\,.\,\overline{f-y}}{\overline{c-x}\,.\,\overline{d-x}\,.\,\overline{e-x}}}\right\},$$

$$\dots \quad \dots \quad \dots \quad \dots \quad \dots \text{ (ten even functions)}.$$

The Greek letters always connote the zero values of the variables: thus $(\alpha\beta)$ is the value of (AB) when $u = 0$, $v = 0$. I also for the sake of greater simplicity usually write (ABF) or (CDE) as the equivalent of (AB); so that I have always, for example,

$$(AB) \equiv (ABF) \equiv (CDE),$$

$$(CD) \equiv (CDF) \equiv (ABE).$$

Further, I shall sometimes use the letters P, Q, R as general representatives of any one of the letters A, B, C, D, E, F.

7. This notation is, of course, in effect, the equivalent of the notation by characteristics, the theta-function (AEF) being merely the function whose characteristic is the sum of the characteristics of A, E, F. There is therefore a corresponding notation for the characteristics of the quarter periods, but it is more convenient to take the fifteen distinct quarter periods as denoted by a symbol of a pair of letters only, *e.g.*, (ef), of which pairs there are, of course, out of six letters fifteen. Then the effect of the addition to the variables u and v of the conjugate quarter periods denoted by (ef) is to add EF to the symbol of the function, and then, with the obvious conventions that $PP = 0$, where P is any one of the six letters, and that $ABCDEF = 0$, the new symbol is at once written down.

For example, the addition of the quarter period (ef) changes A into AEF, AEF into A, ABF into ABE, ABC into D. The fourth root of unity which enters as a coefficient* is troublesome, and may be determined by the following rules.

---

* *Cf.* the table, Cayley, Vol. x., p. 172.

Taking, with Cayley, the correspondence of symbols and characteristics to be

A	B	C	D	E	F
11	11	10	10	01	01
01	10	10	11	11	01

the table

	A	B	C	D	E	F
a, b	ι	ι	ι	$-$	$-$	ι
c, d	$+$	ι	ι	ι	ι	$+$
e, f	ι	$+$	$+$	ι	ι	ι

(18)

gives the multiplier corresponding to each letter in the symbol of a quarter period, when that quarter period is added to the variables u, v.* Further, in reducing the symbol F^2, A^2 with E, F, A, B; B^2, C^2 with A, B, C, D; D^2, E^2 with C, D, E, F, all give a minus sign. The final coefficient is the product of all those taken in this way for the separate letters. Thus, for instance, the quarter period (bc) added to the variables changes A into $\iota\,(ABC)$, (BDE) into (CDE), &c., &c.

It will still be true that a symbol with three letters, *e.g.* (ABF), is exactly equivalent to the symbol with the other three, *e.g.* (CDE).

8. The first result, then, that I obtain [by putting $\lambda = a, b, \ldots$ in (17)] is that, when

$$u_1 \pm u_2 \pm u_3 = 0, \quad v_1 \pm v_2 \pm v_3 = 0,$$

there is a linear relation between any five of the products $P_1 P_2 P_3$ the suffix numbers being used to denote the corresponding arguments. The coefficients are easily determined by giving special values to the u's and v's.

Thus one relation written out in full is

$$\begin{aligned}&(\alpha\beta\zeta)(\alpha\gamma\zeta)(\alpha\delta\zeta)(\alpha\epsilon\zeta)\,A_1A_2A_3-(\alpha\beta\zeta)(\beta\gamma\zeta)(\beta\delta\zeta)(\beta\epsilon\zeta)\,B_1B_2B_3\\&-(\alpha\gamma\zeta)(\beta\gamma\zeta)(\gamma\delta\zeta)(\gamma\epsilon\zeta)\,C_1C_2C_3+(\alpha\delta\zeta)(\beta\delta\zeta)(\gamma\delta\zeta)(\delta\epsilon\zeta)\,D_1D_2D_3\\&+(\alpha\epsilon\zeta)(\beta\epsilon\zeta)(\gamma\epsilon\zeta)(\delta\epsilon\zeta)\,E_1E_2E_3=0.\end{aligned} \quad (19)$$

9. This relation gives at once an interesting expression for the quotient of two Θ-functions of the sum or difference of two arguments. Taking

$$u_3 = u_1 - u_2, \quad v_3 = v_1 - v_2,$$

u_3, v_3 are unaltered by any, the same, additions to u_1, u_2 and v_1, v_2, and in particular by the addition of quarter periods.

---

* *Cf.* Forsyth, *Phil. Trans.*, 1882, Pt. III., pp. 790–1.

Thus, putting P_{12} as an abbreviation for P_1P_2, and $(\overline{a\zeta})$ for $(a\beta\zeta)(a\gamma\zeta)(a\delta\zeta)(a\epsilon\zeta)$, we get

$$\left.\begin{array}{ll}
\text{(i.)} & (\overline{a\zeta})\,A_{12}A_3-(\overline{\beta\zeta})\,B_{12}B_3-(\overline{\gamma\zeta})\,C_{12}C_3+(\delta\zeta)\,D_{12}D_3 \\
& \qquad\qquad +(\overline{\epsilon\zeta})\,E_{12}E_3=0 \\
\text{(ii.)} & (\overline{a\zeta})\,E_{12}A_3+(\overline{\beta\zeta})(ABE)_{12}B_3+(\overline{\gamma\zeta})(ACE)_{12}C_3 \\
& \qquad\qquad -(\overline{\delta\zeta})(ADE)_{12}D_3-(\overline{\epsilon\zeta})\,A_{12}E_3=0 \\
\text{(iii.)} & (\overline{a\zeta})(ABE)_{12}A_3+(\overline{\beta\zeta})\,E_{12}B_3+(\overline{\gamma\zeta})(BCE)_{12}C_3 \\
& \qquad\qquad -(\overline{\delta\zeta})(BDE)_{12}D_3-(\overline{\epsilon\zeta})\,B_{12}E_3=0 \\
\text{(iv.)} & -(\overline{a\zeta})(ACE)_{12}A_3+(\overline{\beta\zeta})(BCE)_{12}B_3+(\overline{\gamma\zeta})\,E_{12}C_3 \\
& \qquad\qquad +(\overline{\delta\zeta})(CDE)_{12}D_3+(\overline{\epsilon\zeta})\,C_{12}E_3=0 \\
\text{(v.)} & -(\overline{a\zeta})(ADE)_{12}A_3+(\overline{\beta\zeta})(BDE)_{12}B_3+(\overline{\gamma\zeta})(CDE)_{12}C_3 \\
& \qquad\qquad +(\delta\zeta)\,E_{12}D_3+(\overline{\epsilon\zeta})\,D_{12}E_3=0
\end{array}\right\},$$

&c. &c. (20)

which give relations of which

$$\frac{(\overline{a\zeta})\,A_3}{\begin{vmatrix} -B_{12}, & -C_{12}, & D_{12}, & E_{12} \\ (ABE)_{12}, & (ACE)_{12}, & -(ADE)_{12}, & -A_{12} \\ E_{12}, & (BCE)_{12}, & -(BDE)_{12}, & -B_{12} \\ (BCE)_{12}, & E_{12}, & (CDE)_{12}, & C_{12} \end{vmatrix}} = \frac{(\overline{\epsilon\zeta})\,E_3}{\begin{vmatrix} A_{12}, & -B_{12}, & -C_{12}, & D_{12} \\ E_{12}, & (ABE)_{12}, & (ACE)_{12}, & -(ADE)_{12} \\ (ABE)_{12}, & E_{12}, & (BCE)_{12}, & -(BDE)_{12} \\ -(ACE)_{12}, & (BCE)_{12}, & E_{12}, & (CDE)_{12} \end{vmatrix}} \qquad (21)$$

is one specimen.

10. The equations (16) and (17) may be used further to give an addition theorem for four arguments. Keeping u_1, v_1, u_2, v_2 the same as before, write

$$\left.\begin{aligned} u_3 &= \int\frac{dx_3}{\sqrt{X_3}}-\int\frac{d\lambda}{\sqrt{\Lambda}} \\ v_3 &= \int\frac{x_3\,dx_3}{\sqrt{X_3}}-\int\frac{\lambda\,d\lambda}{\sqrt{\Lambda}} \end{aligned}\right\}, \qquad (22)$$

where λ may have any value. Then (16) gives

$$\left.\begin{aligned} u_1+u_2+u_3 &= \int\frac{dy_3}{\sqrt{Y_3}}-\int\frac{d\lambda}{\sqrt{\Lambda}} = -u_4, \text{ say} \\ u_1+u_2+u_3 &= \int\frac{y_3\,dy_3}{\sqrt{Y_3}}-\int\frac{\lambda\,d\lambda}{\sqrt{\Lambda}} = -v_4 \end{aligned}\right\}. \tag{23}$$

Thus equation (17) gives an integral of

$$u_1 \pm u_2 \pm u_3 \pm u_4 = 0, \quad v_1 \pm v_2 \pm v_3 \pm v_4 = 0, \tag{24}$$

which may be written

$$\Sigma_P P_1 P_2 P_3 P_4 = \Sigma_Q Q_1 Q_2 Q_3 Q_4 \, (P = A,\, C,\, E;\; Q = B,\, D,\, F).^* \tag{25}$$

11. This relation admits of many transformations and special cases. For example, all the fundamental relations between the squares and products of Θ-functions† can be derived from it with ease. I add a few examples of theorems to which it gives rise.

(1) Taking u_4, v_4 as a quarter period, it follows that there is a linear relation between any four of the products $P_1P_2P_3$ when the sum of the arguments is a quarter period; or, what is, in effect, the same thing, between the products $(PQR)_1(PQR)_2(PQR)_3$, where P takes any four different values, when the sum of the arguments is zero.

From these are deduced, after the manner of (21), relations of which the following is a specimen. If

$$u_3 = u_1 - u_2, \quad v_3 = v_1 - v_2,$$

$$\frac{(\alpha\epsilon\zeta)(AEF)_3}{\begin{vmatrix} B_{12}, & C_{12}, & D_{12} \\ (BEF)_{12}, & (CEF)_{12}, & (DEF)_{12} \\ (BCD)_{12}, & D_{12}, & C_{12} \end{vmatrix}} = \frac{-(\beta\epsilon\zeta)(BEF)_3}{\begin{vmatrix} A_{12}, & C_{12}, & D_{12} \\ (AEF)_{12}, & (CEF)_{12}, & (DEF)_{12} \\ (ACD)_{12}, & D_{12}, & C_{12} \end{vmatrix}}$$

$$= \frac{(\gamma\epsilon\zeta)(CEF)_3}{\begin{vmatrix} A_{12}, & B_{12}, & D_{12} \\ (AEF)_{12}, & (BEF)_{12}, & (DEF)_{12} \\ (ACD)_{12}, & (BCD)_{12}, & C_{12} \end{vmatrix}} = \frac{-(\delta\epsilon\zeta)(DEF)_3}{\begin{vmatrix} A_{12}, & B_{12}, & C_{12} \\ (AEF)_{12}, & (BEF)_{12}, & (CEF)_{12} \\ (ACD)_{12}, & (BCD)_{12}, & D_{12} \end{vmatrix}}. \tag{26}$$

---

[*] This equation is given by Forsyth, "Memoir on the Theta-Functions," *Phil. Trans.*, 1882, Pt. III., p. 845, § 57, as a deduction from the product theorem.

[†] *Cf.* tables in Cayley's memoir, *Coll. Works*, Vol. X., p. 544, &c.

It is interesting to notice the direct correspondence with the elliptic function formulæ of the type

$$\operatorname{dn}(u_1-u_2) = \begin{vmatrix} c_1c_2, & k'^2 \\ s_1s_2, & d_1d_2 \end{vmatrix} \div \begin{vmatrix} c_1c_2, & d_1d_2 \\ s_1s_2, & 1 \end{vmatrix}.$$

(2) For any pair of arguments

$$A_1^2A_2^2-B_1^2B_2^2+C_1^2C_2^2-D_1^2D_2^2+E_1^2E_2^2-F_1^2F_2^2 = 0, \tag{27}$$

and for any argument

$$A^4-B^4+C^4-D^4+E^4-F^2 = 0. \tag{28}$$

12. The extension of the method of this paper to the hyperelliptic functions of any order is immediate. Thus, for instance, for hyperelliptic triple Θ-functions we must take confocal ${}_5R_7$'s in a space S_7 given by

$$\Sigma \frac{x_\iota^2}{a_\iota+\lambda}-1 = 0 \quad \begin{pmatrix} \iota = 1, 2, 3, 4, 5, 6, 7; \\ \lambda = p, q, r, s, t, u, v \end{pmatrix}.$$

There will be three surfaces, T, U, V, say, corresponding to equations (6), § 2, and three tangent ${}_1R_6$'s corresponding to (7).

Then equation (8) will have seven terms, and for (9) and (10) we must substitute

$$\xi_t = 0, \quad \xi_u = 0, \quad \xi_v = 0,$$

$$\frac{\xi_p^2}{p-t}+\frac{\xi_q^2}{q-t}+\frac{\xi_r^2}{r-t}+\frac{\xi_s^2}{s-t} = 0,$$

$$\frac{\xi_p^2}{p-u}+\frac{\xi_q^2}{q-u}+\frac{\xi_r^2}{r-u}+\frac{\xi_s^2}{s-u} = 0,$$

$$\frac{\xi_p^2}{p-v}+\frac{\xi_q^2}{q-v}+\frac{\xi_r^2}{r-v}+\frac{\xi_s^2}{s-v} = 0,$$

giving, as before,

$$\frac{\xi_p^2}{(p-t)(p-u)(p-v)(q-r)(r-s)(s-q)}$$

$$= \frac{\xi_q^2}{(q-t)(q-u)(q-v)(r-s)(s-p)(p-r)} = \text{\&c., \&c.,}$$

and then, with $f(\theta) = \Theta = \Pi_\iota\,(a_\iota+\theta) \quad (\iota = 1, 2, \ldots, 7)$,

$$\frac{1}{(q-r)(r-s)(s-q)}\,\frac{dp}{\sqrt{P}} = \pm\frac{1}{(r-s)(s-p)(p-r)}\,\frac{dq}{\sqrt{Q}} = \text{\&c., \&c.,}$$

and, finally,

$$\frac{\sqrt{p}}{dP}+\epsilon\frac{dq}{\sqrt{Q}}+\epsilon'\frac{dr}{\sqrt{R}}+\epsilon''\frac{ds}{\sqrt{S}}=0,$$

$$\frac{p\,dp}{\sqrt{P}}+\epsilon\frac{q\,dq}{\sqrt{Q}}+\epsilon'\frac{r\,dr}{\sqrt{R}}+\epsilon''\frac{s\,ds}{\sqrt{S}}=0,$$

$$\frac{p^2dp}{\sqrt{P}}+\epsilon\frac{q^2dq}{\sqrt{Q}}+\epsilon'\frac{r^2dr}{\sqrt{R}}+\epsilon''\frac{s^2ds}{\sqrt{S}}=0.$$

Then the equations corresponding to (14) will have eight terms, and the corresponding integral will be

$$\Sigma_\iota\frac{(a_\iota+\lambda)(a_\iota+\mu)\sqrt{a_\iota+p\,.\,a_\iota+p_0\,.\,a_\iota+q\,.\,a_\iota+q_0\,.\,a_\iota+r\,.\,a_\iota+r_0\,.\,a_\iota+s\,.\,a_\iota+s_0}}{f'(-a_\iota)}=1.$$

13. It appears from this that the results of § 8 do not apply for hyperelliptic functions of odd order, but only for those of even order.

The results of § 10 (and those of § 8 when the order is even) will, however, follow by adding and subtracting

$$\int\frac{d\lambda}{\sqrt{\Lambda}}+\int\frac{d\mu}{\sqrt{\mathrm{M}}},\quad\int\frac{\lambda\,d\lambda}{\sqrt{\Lambda}}+\int\frac{\mu\,d\mu}{\sqrt{\mathrm{M}}},\quad\int\frac{\lambda^2d\lambda}{\sqrt{\Lambda}}+\int\frac{\mu^2d\mu}{\sqrt{\mathrm{M}}}$$

as required for the triple functions, and corresponding changes for any order.

In fact, when the order is p, the sum of $2p+2$ integrals will be obtained by the geometrical method, and this can be increased to $4p$ for all values of p, and also to $3p$ when p is even.

14. For the hyperelliptic triple Θ-functions I get, putting

$$\Theta=a-\theta\,.\,b-\theta\,.\,c-\theta\,.\,d-\theta\,.\,e-\theta\,.\,f-\theta\,.\,g-\theta\,.\,h-\theta,$$

that

$$\left.\begin{aligned}\Sigma_\iota\left(\int\frac{dx_\iota}{\sqrt{X_\iota}}+\int\frac{dy_\iota}{\sqrt{Y_\iota}}+\int\frac{dz_\iota}{\sqrt{Z_\iota}}\right)&=0\\\Sigma_\iota\left(\int\frac{x_\iota dx}{\sqrt{X_\iota}}+\int\frac{y_\iota dy}{\sqrt{Y_\iota}}+\int\frac{z_\iota dz_\iota}{\sqrt{Z_\iota}}\right)&=0\\\Sigma_\iota\left(\int\frac{x_\iota^2dx_\iota}{\sqrt{X_\iota}}+\int\frac{y_\iota^2dy_\iota}{\sqrt{Y_\iota}}+\int\frac{z_\iota^2dz_\iota}{\sqrt{Z_\iota}}\right)&=0\end{aligned}\right\}\quad(\iota=1,2,3,4);$$

have an integral

$$\Sigma_s\frac{\Pi_\iota\sqrt{s-x_\iota\,.\,s-y_\iota\,.\,s-z_\iota}}{\dfrac{dS}{ds}}=0,$$

$$(s=a,b,c,d,e,f,g,h;\quad\iota=1,2,3,4).$$

Thursday, January 10th, 1901.

Dr. HOBSON, F.R.S., President, in the Chair.

Fourteen members present and two visitors.

Mr. Harold W. Curjel, M.A., Southport, and Mr. G. H. Hardy, B.A., Fellow of Trinity College, Cambridge, were elected members, and Mr. H. W. Richmond was admitted into the Society.

Prof. Love spoke "On Streaming Motions past Cylindrical Boundaries." Mr. Basset also spoke on the subject.

Mr. Campbell read a paper entitled "A Proof of the Third Fundamental Theorem in Lie's Theory of Continuous Groups."

The President communicated papers by Mr. Barnes "On the Zeroes of Bessel's Functions," and by Prof. Carey "On some cases of the Solution of $z^{p^n-1} \equiv 1$, mod p."

The following presents were made to the Library :—

"Mathematical Gazette," Vol. I., No. 24, Vol. II., No. 1 ; 1901.

"Royal Society, Reports to the Malaria Committee," 8vo ; London, 1900.

"Transactions of the Literary and Scientific Society," No. 2 ; Ottawa, 1899-1900.

"Transactions of the American Mathematical Society," Vol. I , No. 4 ; 1900.

His, W.—"Lecithoblast und Angioblast der Wirbelthiere," roy. 8vo ; Leipzig, 1900.

"Educational Times," Jan., 1901.

"Indian Engineering," Vol. XXVIII., Nos. 21-24, Nov. 24-Dec. 15, 1900.

The following exchanges were received :—

"Proceedings of the Royal Society," Vol. LXVII., No. 439 ; 1901.

"Beiblätter zu den Annalen der Physik und Chemie," Bd. XXIV., St. 11 ; Leipzig, 1900.

"Bulletin of the American Mathematical Society," Series 2, Vol. VII., No. 3 ; New York, 1900.

"Monatshefte für Mathematik und Physik," Jahrgang XII., Pt. 1 ; Wien, 1901.

"Atti della Reale Accademia dei Lincei—Rendiconti," Sem. 2, Vol. IX., Fasc. 11 ; Roma, 1900.

"Berichte über die Verhandlungen der Königl. Sächs. Gesellschaft der Wissenschaften zu Leipzig," Bd. LII., No. 6 ; 1900.

"Nyt Tidsskrift for Matematik," B. Aargang XI., Nr. 4 ; Copenhagen, 1900.

"Proceedings of the Physical Society," Vol. XVII., Pt. 4 ; Dec., 1900.

"Jahrbuch über die Fortschritte der Mathematik," Bd. XXIX., Heft 3 ; Berlin, 900.

Proof of the Third Fundamental Theorem in Lie's Theory of Continuous Groups. *By* J. E. CAMPBELL.

Read January 10th, 1901. Received January 12th, 1901.

If we have any set of r^3 constants, $c_{ih\kappa}$ ..., satisfying the conditions

$$c_{i\kappa h}+c_{\kappa i h}=0,$$

$$\sum_{h=1}^{h=r}(c_{i\kappa h}c_{hjt}+c_{\kappa jh}c_{hit}+c_{jih}c_{h\kappa t})=0$$

$$(i,\ \kappa,\ j,\ t=1,\ \ldots,\ r), \qquad (1)$$

they are said to form a set of composition constants of the r-th order; and the third fundamental theorem in Lie's theory of continuous groups is that, given any such set, r independent infinitesimal transformations

$$X_1,\ \ldots,\ X_r$$

can be found, such that

$$X_iX_\kappa-X_\kappa X_i=c_{i\kappa 1}X_1+\ldots+c_{i\kappa r}X_r\,;$$

and therefore such that they generate a group of the given composition.

Lie gives a proof of this proposition in the second volume (seventeenth chapter) of *Transformationsgruppen*, but it requires a considerable previous knowledge of his theory of function groups to follow it; and a proof has also been given by Herr Schur, which is sketched in the third volume, § 144. Recently M. Poincaré has discussed the theorem in the *Trans. of the Camb. Phil. Soc.*, Vol. XVIII., p. 234, and given a proof of the soundness of which I do not feel sure. He has shown how to construct r infinitesimal transformations which are independent; to verify their group property is not easy, and would, in effect, be Schur's method; if this property is not verified independently, the reasoning which occurs on p. 234—" Let

$$e^Ve^T=e^W,\quad e^We^U=e^Z,\quad e^Te^U=e^Y,$$

where $\qquad U=\Sigma u_\kappa X_\kappa,\quad Z=\Sigma z_\kappa X_\kappa,\quad Y=\Sigma y_\kappa X_\kappa\,;$

the associative character of the operations shows us that we have

$$e^Ve^Y=e^Z,$$

where
$$w_\kappa = \phi_\kappa(v_i, t_i), \quad y_\kappa = \phi_\kappa(t_i, u_i),$$
$$Z_\kappa = \phi_\kappa(w_i, u_i) = \phi_\kappa(v_i, y_i)\text{''}$$
—seems to presuppose the existence of a group of the required composition.

If it is objected that we can let $X_1 \ldots X_r$ be the group adjoint, then, unless these operators are independent, we do not know that the associative law holds.

The proof given here is perhaps simpler than those to which I have referred, with the exception of M. Poincaré's, if the latter is correct; in any case the proposition is so important that it may perhaps justify one in giving another proof.

Since writing this paper my attention has been drawn by one of the referees to a proof of this theorem by Klein, in his *Einleitung in die höhere Geometrie*, Vol. II., pp. 163–167, which at first is on the same lines as the proof of this paper, viz., the replacing of the given composition constants by an equivalent but simpler set when the adjoint group is of order less than r. I believe that this proof is erroneous; perhaps the simplest reason for doubting it is that, if correct, it would (as the referee remarked) prove that a group which contains self-conjugate (*ausgereichnete*) operations must be the direct product of two independent groups. Klein assumes, in fact, that the constants which in § 5 I have denoted by $d_{i\kappa m} \ldots$ are all zero. I might perhaps add here that the results in §§ 1–3 of my paper are implicitly contained in chapter XVII. of the first volume of the *Transformationsgruppen*.

1. If
$$x_i = \sum_{\kappa=1}^{\kappa=r} a_{\kappa i} x'_\kappa \quad (i = 1, \ldots, r)$$
is any linear transformation whose modulus does not vanish, and
$$x'_i = \sum_{\kappa=1}^{\kappa=r} A_{\kappa i} x_\kappa$$
the inverse transformation, then $c_{i\kappa h} \ldots$ being any r^3 other set of variables, and $c'_{i\kappa h} \ldots$ another set connected with the former by the equations
$$\sum_{h=1}^{h=r} a_{hs} c'_{i\kappa h} = \sum_{pq} a_{ip} a_{\kappa q} c_{pqs} \tag{2}$$
(the summation on the right being for all values of p, q from 1 up to r inclusive, and i, κ, s having any values from 1 up to r inclusive), it is clear that (2) gives $c'_{i\kappa h} \ldots$ in terms of $c_{i\kappa h} \ldots$.

From the fact that $\sum_{p=1}^{p=r} A_{pi} a_{\kappa p} = \epsilon_{i\kappa}$,

where $\epsilon_{i\kappa}$ is zero if $i \neq \kappa$, and unity if $i = \kappa$, we easily verify that

$$\sum_{h=1}^{h=r} A_{hs} c_{i\kappa h} = \sum_{pq} A_{ip} A_{\kappa q} c'_{pqs} ;$$

and therefore $c_{i\kappa h}$ ... are given in terms of $c'_{i\kappa h}$ ... .

2. It must now be proved that, if one set $c_{i\kappa h}$ ... satisfy the system of equations (1), so will the other $c'_{i\kappa h}$ ... .

To see this, multiply (2) by $a_{tm} c_{smj}$, and sum for all values of h, s, m, p, q, and we get

$$\sum_{h,\, s,\, m} a_{hs} a_{tm} c'_{i\kappa h} c_{smj} = \sum_{m,\, s,\, p,\, q} a_{ip} a_{\kappa q} a_{tm} c_{pqs} c_{smj} .$$

Noticing that by (2) the left-hand member may be written

$$\sum_{m,\, h} a_{mj} c'_{i,\, \kappa,\, h} c'_{h,\, t,\, m},$$

we see that $\sum_{m=1}^{m=r} a_{mj} \sum_{h=1}^{h=r} (c'_{i\kappa h} c'_{htm} + c'_{\kappa th} c'_{him} + c'_{t,\, i,\, h} c'_{h,\, \kappa,\, m})$

is the sum of a number of terms which vanish by the conditions (1).

We conclude therefore that, since the modulus does not vanish,

$$\sum_{h=1}^{h=r} (c'_{i\kappa h} c'_{htm} + c'_{\kappa th} c'_{him} + c'_{tih} c'_{h\kappa m}) = 0$$

for all values of i, κ, m, t.

To prove that $c'_{i\kappa t} + c'_{\kappa it} = 0$,

interchange i, κ in (2); we get

$$\sum_{h=1}^{h=r} a_{hs} c'_{\kappa ih} = \sum_{pq} a_{iq} a_{\kappa p} c_{pqs} ;$$

adding this equation and (2), we see that

$$c'_{i\kappa t} + c'_{\kappa it} = 0$$

from conditions (1).

3. Suppose now that we have a group with the composition constants $c_{i\kappa h}$ ..., the corresponding infinitesimal transformations being X_1, ..., X_r.

If we take X'_1, ..., X'_r as a new set of r independent infinitesimal transformations defined by

$$X'_i = \sum_{\kappa=1}^{\kappa=r} a_{i\kappa} X_\kappa ,$$

then it can be at once verified that $c'_{\iota\kappa h}$ ... are the composition constants of the group corresponding to the above infinitesimal transformations; the conclusion we draw is that when we can find a group with the composition constants $c_{\iota\kappa h}$ ... it has also the composition constants $c'_{\iota\kappa h}$ ..., and conversely.

4. Suppose now we are given a set of composition constants $c_{ih\kappa}$ ..., such that all $r-s+1$ rowed determinants, but not all $r-s$ rowed determinants, vanish of the matrix

$$\begin{vmatrix} c_{j1\kappa} & \cdots \\ c_{j2\kappa} & \cdots \\ \vdots & \cdots \\ c_{jr\kappa} & \cdots \end{vmatrix}$$

(in any row all positive integral values of j and κ are to be taken from 1 up to r); then we can choose

$$\begin{matrix} a_{11}, \ldots, a_{1r}, \\ a_{21}, \ldots, a_{2r}, \\ \vdots \\ a_{s1}, \ldots, a_{sr} \end{matrix}$$

so that $$a_{h1}c_{j1\kappa}+a_{h2}c_{j2\kappa}+\ldots+a_{hr}c_{jr\kappa}=0,$$

where j, κ may have any values from 1 up to r inclusive, and h any value from 1 up to s inclusive.

To complete the determinant of the $a_{p,q}$'s we can take $a_{m\kappa}$ arbitrarily, only providing that the determinant does not vanish ($m=s+1, \ldots, r$; $\kappa=1, \ldots, r$).

If we now apply the transformation (2), we get a new set of composition constants $c'_{\iota\kappa h}$ with the property

$$c'_{\iota\kappa h}=d_{\iota\kappa h},$$

where i, κ, h may have any values from $s+1$ up to r, and $d_{\iota\kappa h}$ are a set of composition constants of the n-th order, n being written for $r-s$;

$$c'_{\iota\kappa h}=0,$$

if either i or κ is less than $s+1$, h having any value from 1 up to

r inclusive;

$$c'_{\iota\kappa m},$$

where ι and κ both exceed s, and m does not, being such that

$$c'_{\iota\kappa m}+c'_{\kappa\iota m}=0,$$

$$\sum_{h=s+1}^{h=r}\left(d_{\iota\kappa h}c'_{hjm}+d_{\kappa jh}c'_{h\iota m}+d_{j\iota h}c'_{h\kappa m}\right)=0.$$

5. We may therefore say (with the slight change of notation which consists in writing $d_{\iota\kappa h}=c_{r-\iota,r-\kappa,r-h}$ and $c'_{\iota\kappa m}=d_{r-\iota,r-\kappa,r-m}$) that the problem of finding a group with the given composition is now reduced to that of finding a group with the composition constants

$$d'_{\iota\kappa h}\,\ldots,$$

where

$$d'_{\iota\kappa h}=c_{\iota\kappa h},$$

if none of the suffixes ι, κ, h exceed n, and the c's are composition constants of the n-th order, such that not all n rowed determinants vanish of the matrix

$$\left\|\begin{matrix} c_{j1\kappa} & \ldots \\ c_{j2\kappa} & \ldots \\ \vdots & \\ c_{jn\kappa} & \ldots \end{matrix}\right\| \quad (j,\kappa=1,\ldots,n)\,; \tag{3}$$

$$d'_{\iota\kappa h}=0,$$

if either ι or κ exceeds n, h having any value from 1 up to r;

$$d'_{\iota\kappa m}=d_{\iota\kappa m},$$

if neither ι nor κ exceeds n, and m does exceed n, and

$$d_{\iota\kappa m}+d_{\kappa\iota m}=0,$$

$$\sum_{h=1}^{h=n}\left(c_{\iota\kappa h}d_{hjm}+c_{\kappa jh}d_{h\iota m}+c_{j\iota h}d_{h\kappa m}\right)=0. \tag{4}$$

Now, it may at once be verified that

$$X_1,\ldots,X_n,$$

where

$$X_i=\sum_{pq}c_{piq}x_p\frac{\partial}{\partial x_q}$$

(the summation being for all values of p and q from 1 up to n inclusive), is a group of the n-th order with the composition constants $c_{ih\kappa}$; for, by (3), $X_1,\ldots,X_n$ are independent, and by forming its alternants we verify the group property. This is Lie's group adjoint. Its parameter group is simply transitive and of like composition with it; we have therefore proved the existence of a simply transitive group with the composition constants $c_{i\kappa h}$ ... .

6. It will now be shown how a simply transitive group with the composition constants $d'_{i\kappa h}$ ... may be deduced.

Let $X_1, \ldots, X_n$ be the simply transitive group with the composition constants $c_{i\kappa h}$ ... .

Let $u_{1m}, u_{2m}, \ldots, u_{nm}$ be any set of solutions of the simultaneous equation system

$$X_i u_{\kappa m} - X_\kappa u_{im} = d_{i\kappa m} + \sum_{h=1}^{h=n} c_{i\kappa h} u_{hm}, \tag{5}$$

where i, κ may have all values from 1 up to n, and m has all values from $n+1$ up to r. We can at once verify that

$$X_i + u_{i\,n+1}\frac{\partial}{\partial x_{n+1}} + \ldots + u_{ir}\frac{\partial}{\partial x_r} \quad (i = 1, \ldots, n),$$

$$\frac{\partial}{\partial x_{n+1}}, \ldots, \frac{\partial}{\partial x_r},$$

is a simply transitive group of order r with the composition constants $d'_{i\kappa h}$ ... .

7. We must now prove that the equation system (5) is self-consistent. This may be done by the method explained in the *Proc. of the Lond. Math. Soc.*, Vol. XXXI., p. 235, or independently by a less general but more direct method as follows:—

Since $X_1, \ldots, X_n$ is a simply transitive group, $\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}$ can each be expressed in the form

$$\frac{\partial}{\partial x_i} = \lambda_{1i} X_1 + \ldots + \lambda_{ni} X_n,$$

where $\lambda_{i\kappa}$ ... are a known set of functions in $x_1, \ldots, x_n$. From the fact that

$$\frac{\partial}{\partial x_i}\frac{\partial}{\partial x_\kappa} = \frac{\partial}{\partial x_\kappa}\frac{\partial}{\partial x_i},$$

and that $X_1, \ldots, X_n$ form a group, we see that $\lambda_{i\kappa}$ ... are functions satisfying the equation system

$$\frac{\partial \lambda_{j\kappa}}{\partial x_i} - \frac{\partial \lambda_{ji}}{\partial x_\kappa} = \sum_{\alpha,\beta} c_{\alpha\beta j}\lambda_{\alpha\kappa}\lambda_{\beta i} \tag{6}$$

(the summation being for all values of α, β from 1 up to n inclusive).

8. It must first be verified that

$$\frac{\partial}{\partial x_i} \Sigma\, d_{\alpha\beta m} \lambda_{\alpha j} \lambda_{\beta\kappa} + \frac{\partial}{\partial x_j} \Sigma\, d_{\alpha\beta m} \lambda_{\alpha\kappa} \lambda_{\beta i} + \frac{\partial}{\partial x_\kappa} \Sigma\, d_{\alpha\beta m} \lambda_{\alpha i} \lambda_{\beta j} \tag{7}$$

is identically zero for all values of $ij\kappa$, the summation in Σ being for all values of α, β. We have

$$\frac{\partial}{\partial x_i} \lambda_{\alpha j} \lambda_{\beta\kappa} = \lambda_{\alpha j} \frac{\partial}{\partial x} \lambda_{\beta\kappa} + \lambda_{\beta\kappa} \frac{\partial}{\partial x_i} \lambda_{\alpha i},$$

$$\frac{\partial}{\partial x_j} \lambda_{\alpha\kappa} \lambda_{\beta i} = \lambda_{\alpha\kappa} \frac{\partial}{\partial x_j} \lambda_{\beta i} + \lambda_{\beta i} \frac{\partial}{\partial x_j} \lambda_{\alpha\kappa},$$

$$\frac{\partial}{\partial x_\kappa} \lambda_{\alpha i} \lambda_{\beta j} = \lambda_{\alpha i} \frac{\partial}{\partial x_\kappa} \lambda_{\beta j} + \lambda_{\beta j} \frac{\partial}{\partial x_\kappa} \lambda_{\alpha i}.$$

Remembering that $\qquad d_{\alpha\beta m} + d_{\beta\alpha m} = 0,$

we see that (7) may be written

$$\sum_{\alpha,\beta} \lambda_{\alpha j} d_{\alpha\beta m} \left(\frac{\partial}{\partial x_i} \lambda_{\beta\kappa} - \frac{\partial}{\partial x_\kappa} \lambda_{\beta i} \right) + \sum_{\alpha,\beta} \lambda_{\beta\kappa} d_{\alpha\beta m} \left(\frac{\partial}{\partial x_i} \lambda_{\alpha j} - \frac{\partial}{\partial x_j} \lambda_{\alpha i} \right)$$
$$+ \sum_{\alpha,\beta} \lambda_{\beta i} d_{\alpha\beta m} \left(\frac{\partial}{\partial x_j} \lambda_{\alpha\kappa} - \frac{\partial}{\partial x_\kappa} \lambda_{\alpha j} \right).$$

Writing the second and third of these sums in the equivalent forms

$$\sum_{\gamma,\beta} \lambda_{\gamma,\kappa}\, d_{\gamma,\beta m} \left(\frac{\partial}{\partial x_j} \lambda_{\beta i} - \frac{\partial}{\partial x_i} \lambda_{\beta j} \right)$$

and

$$\sum_{b,\beta} \lambda_{bi}\, d_{b\beta m} \left(\frac{\partial}{\partial x_\kappa} \lambda_{\beta j} - \frac{\partial}{\partial x_j} \lambda_{\beta\kappa} \right),$$

and substituting from (6), we see that the coefficient of $\lambda_{aj}\lambda_{\gamma\kappa}\lambda_{bi}$ in (7) is

$$-\sum_{\beta=1}^{\beta=n} \left(d_{\beta am} c_{\gamma b\beta} + d_{\beta am} c_{b\gamma\beta} + d_{\beta bm} c_{a\gamma\beta} \right),$$

which is zero from (4); and therefore, since all these coefficients vanish, the identical relation required is now proved.

9. In order to prove that the simultaneous equation system (5) can be satisfied, multiply (5) by $\lambda_{ip}\lambda_{\kappa q}$, and sum for all values of i, κ; then, if the new set of equations—there will be one for each pair of values of pq—can be satisfied, so can the old; to see this we have only to notice that for the equation with a given pair of [illegible] of i, κ the multiplier is $\lambda_{ip}\lambda_{\kappa q} - \lambda_{\kappa p}\lambda_{iq}$, and the determinan

cannot vanish since the determinant of λ_{pq} does not vanish (Forsyth, *Differential Equations*, § 212).

Let $$v_{im} = \lambda_{1i}u_{1m} + \dots + \lambda_{ni}u_{nm} \quad (i = 1, \dots n)\,;$$
then the simultaneous equation system takes the simple form
$$\frac{\partial}{\partial x_p} v_{qm} - \frac{\partial}{\partial x_q} v_{pm} = \sum_{i\kappa} d_{i\kappa m}\lambda_{ip}\lambda_{\kappa q} = \sigma_{pqm}, \text{ say.} \tag{8}$$

10. To solve these equations, consider the following lemma:—

If we have $\frac{n(n-1)}{2}$ functions $\sigma_{i\kappa}\dots$ of the variables $x_1, \dots, x_n$ such that
$$\sigma_{i\kappa} + \sigma_{\kappa i} = 0,$$
$$\frac{\partial}{\partial x_i}\sigma_{j\kappa} + \frac{\partial}{\partial x_j}\sigma_{\kappa i} + \frac{\partial}{\partial x_\kappa}\sigma_{ij} = 0,$$
where the suffixes may have any values from 1 up to n inclusive, then n functions $u_1, \dots, u_n$ can be found such that
$$\sigma_{i\kappa} = \frac{\partial^2}{\partial x_i \partial x_\kappa}(u_i - u_\kappa).$$

To see that this is true when $n = 3$, let
$$\sigma_{12} = \frac{\partial^2}{\partial x_1 \partial x_2}(u_2 - u_2), \quad \sigma_{13} = \frac{\partial^2}{\partial x_1 \partial x_3}(u_1 - u_3).$$
This is clearly justifiable, and we can take u_1 arbitrarily and obtain u_2 and u_3 by integration.

Since $$\sigma_{12} + \sigma_{21} = 0 \quad \text{and} \quad \sigma_{13} + \sigma_{31} = 0,$$
$$\sigma_{21} = \frac{\partial^2}{\partial x_1 \partial x_2}(u_2 - u_1), \quad \sigma_{31} = \frac{\partial^2}{\partial x_1 \partial x_3}(u_3 - u_1).$$

Now $$\frac{\partial}{\partial x_1}\sigma_{23} + \frac{\partial}{\partial x_2}\sigma_{31} + \frac{\partial}{\partial x_3}\sigma_{12} = 0\,;$$

therefore $$\frac{\partial}{\partial x_1}\sigma_{23} + \frac{\partial^3}{\partial x_1 \partial x_2 \partial x_3}(u_3 - u_2) = 0,$$

and therefore $$\sigma_{23} = \frac{\partial^2}{\partial x_2 \partial x_3}(u_2 - u_3) + f(x_2, x_3).$$

It is clear that we can write $f(x_2, x_3)$ in the form
$$f = \frac{\partial^2}{\partial x_2 \partial x_3}(w_2 - w_3),$$
where w_2 and w_3 are functions of x_2, x_3 only, and w_2 can be taken

arbitrarily and then w_3 be obtained by integration; therefore

$$\sigma_{23} = \frac{\partial^2}{\partial x_2 \partial x_3}(u_2+w_2-u_3-w_3).$$

Since, then, u_2 and w_3 do not involve x_1, we see that u_1, u_2+w_2, u_3+w_3 are three functions in terms of which σ_{23}, σ_{31}, and σ_{12} can be expressed in the required form.

The extension to n variables is now obvious. Assuming that the theorem has been proved for the case of $n-1$ variables, let

$$\sigma_{1\kappa} = \frac{\partial^2}{\partial x_1 \partial x_\kappa}(u_1-u_\kappa) \qquad (\kappa = 1, \ldots, n),$$

where, as before, u_1 is arbitrary.

From $$\frac{\partial}{\partial x_1}\sigma_{\kappa h} + \frac{\partial}{\partial x_\kappa}\sigma_{h1} + \frac{\partial}{\partial x_h}\sigma_{1\kappa} = 0$$

we get $$\frac{\partial}{\partial x_1}\sigma_{\kappa h} = \frac{\partial^3}{\partial x_1 \partial x_\kappa \partial x_h}(u_\kappa - u_h),$$

and therefore $$\sigma_{\kappa h} = \frac{\partial^2}{\partial x_\kappa \partial x_h}(u_\kappa - u_h) + \rho_{\kappa h},$$

where $\rho_{\kappa h}$ is a function of $x_2, \ldots, x_n$, only.

We now have $$\rho_{\kappa h} + \rho_{h\kappa} = 0,$$

$$\frac{\partial}{\partial x_i}\rho_{h} + \frac{\partial}{\partial x_h}\rho_{\kappa i} + \frac{\partial}{\partial x}\rho_{ih} = 0 \quad (i, h, k = 2, \ldots, n);$$

and therefore, since we now have only $n-1$ variables,

$$\rho_{\kappa h} = \frac{\partial^2}{\partial x_h \partial x_\kappa}(w_\kappa - w_h),$$

where $w_2, \ldots, w_n$ do not involve x_1.

It follows, as before, that

$$u_1,\ u_2+w_2,\ \ldots,\ u_n+w_n$$

will be a set of functions in terms of which we can express in the required manner $\sigma_{\iota\kappa}$ ....

We can now write down the solutions of (8); for we have

$$\sigma_{\iota\kappa m} + \sigma_{\kappa \iota m} = 0,$$

$$\frac{\partial}{\partial x_i}\sigma_{j\kappa m} + \frac{\partial}{\partial x_j}\sigma_{\kappa i m} + \frac{\partial}{\partial x_\kappa}\sigma_{ijm} = 0;$$

the first being true, since $d_{\iota\kappa m} + d_{\kappa\iota m} = 0$, and the secon merely the identity (7); and therefore by the above reasoning we can write

$$\sigma_{i\kappa m} = \frac{\partial^2}{\partial x_i \partial x_\kappa}(V_{im} - V_{\kappa m}),$$

where $V_{i\kappa}$ ... are a set of functions obtainable by quadratures; then

$$v_{im} = -\frac{\partial}{\partial x_i} V_{im}$$

is clearly a system of solutions of the system (8).

We have thus proved that, given any set of composition constants, we can in all cases obtain a simply transitive group of that composition; and that the process of obtaining it involves merely algebraic operations and quadratures.

On some cases of the Solution of the Congruence $z^{p^n-1} \equiv 1$, mod p.

By F. S. Carey. Received January 2nd, 1901. Communicated January 10th, 1901.

Let p be a prime, and x, y integers chosen from amongst

$$0, \pm 1, \pm 2, \ldots, \pm \tfrac{1}{2}(p-1);$$

further, let j be a quantity such that j^2 is congruent to a certain selected quadratic non-residue of p; then $x+yj$ is a symbol which includes p^2 numbers; also for the same modulus p all such numbers are represented by a single j; to prove this, it is sufficient to remark that, if b_1 and b_2 are two quadratic non-residues, and $b_1 = j_1^2$, $b_2 = j_2^2$, then, since $b_1 \equiv a^2 b_2$, it follows that $j_1 = aj_2$ and the p^2 numbers $x+yj_1$ are identical with the p^2 numbers $x+yj_2$. In case $p = 4n+1$, -1 is a non-residue, and the symbol i is used instead of j.

The objects of this paper are (1) to discuss the solution of $z^{p^2} \equiv z$,* mod p, by means of the numbers $x+yj$; (2) to discuss the solution of $z^{p^n} \equiv z$, when p^2-1 is divisible by n; (3) to examine the reduction of the solution in certain other cases in which p^r-1 is divisible by n.

---

* Reference may be made to Serret, *Cours d'Algèbre supérieure*, section iii., chapter iii.

1. The roots of $z^{p^2}\equiv z$, mod p, are the p^2 numbers $x+yj$. For

$$(x+yj)^p\equiv x^p+y^pj^p\equiv x+yb^{\frac{1}{2}(p-1)}j\equiv x-yj,$$

$$(x+yj)^{p^2}\equiv (x-yj)^p\equiv x+yj.$$

If the root zero is excluded from consideration, the (p^2-1) roots of $z^{p^2-1}\equiv 1$ may be divided into two classes, one of which consists of the roots of $z^{\frac{1}{2}(p^2-1)}\equiv 1$, and are quadratic residues, while the others are the roots of $z^{\frac{1}{2}(p^2-1)}\equiv -1$, and are non-residues. As in the theory of real quadratic residues, the product of two residues is a residue, as also is that of two non-residues; while the product of a residue and a non-residue is a non-residue. There are $p(p-1)$ primitive roots of $z^{p^2-1}\equiv 1$; if G be one of these, the whole series of (p^2-1) numbers $x+yj$ is given by

$$1,\ G,\ G^2,\ \ldots,\ G^{p^2-2}.$$

The other primitive roots are the powers of G whose indices are prime to (p^2-1).

A table is given below which contains a series of remainders corresponding to a selected complex primitive root for all values of p less than 100.

To find a primitive root of $z^{p^2-1}\equiv 1$, it is convenient to consider a classification of the (p^2-1) numbers $x+yj$ according to the magnitudes of their norms, and in particular to consider those numbers whose norms are unity.

The norm of each of the following numbers is positive unity:

$$1,\ -1,\ \frac{(1+j)^2}{1-j^2},\ \frac{(2+j)^2}{2^2-j^2},\ \ldots,\ \frac{(p-1+j)^2}{(p-1)^2-j^2}. \tag{A}$$

These numbers are all different, for, if

$$\frac{(c+j)^2}{c^2-j^2}\equiv\frac{(d+j)^2}{d^2-j^2},$$

where $$j^2\equiv b \quad\text{and}\quad c\not\equiv d,$$

then $(c^2+b)(d^2-b)\equiv(c^2-b)(d^2+b)$ and $c(d^2-b)\equiv d(c^2-b)$;

whence it follows that

$$c^2\equiv d^2 \quad\text{and}\quad cd\equiv -b,$$

which are not consistent with themselves, and

$$c\not\equiv d.$$

Again, the numbers in (A) are the roots of $z^{p+1} \equiv 1$. For

$$\left[\frac{(c+j)^2}{c^2-j^2}\right]^p \equiv \frac{(c+j)^{2p}}{(c^2-b)^p} \equiv \frac{(c^p+j^p)^2}{c^{2p}-b^p} \equiv \frac{(c-j)^2}{c^2-b};$$

whence $$\left[\frac{(c+j)^2}{c^2-j^2}\right]^{p+1} \equiv \frac{(c-j)^2(c+j)^2}{(c^2-b)^2} \equiv 1.$$

Let ϵ be a primitive root of $z^{p+1} \equiv 1$; then the numbers in the series (A) can be arranged thus:

$$1,\ \epsilon,\ \epsilon^2,\ \ldots,\ \epsilon^p. \tag{B}$$

Also, if a is an integer not congruent to unity, positive or negative,

$$a,\ a\epsilon,\ a\epsilon^2,\ \ldots,\ a\epsilon^p \tag{C}$$

is a series of non-congruent numbers whose norms are all a^2; indeed, the terms in (C) are the roots of

$$z^{p+1} = a^2.$$

If $p = 4n+1$, the series of numbers (B) and (C) do not contain j; for the norm of j is equal to $-j^2 \equiv -b$, a non-residue. Therefore the series

$$j,\ \epsilon j,\ \epsilon^2 j,\ \ldots,\ \epsilon^p j, \tag{D}$$

$$aj,\ a\epsilon j,\ a\epsilon^2 j,\ \ldots,\ a\epsilon^p j \tag{E}$$

consist of numbers different from the numbers in the series (B) and (C). Now, if all the values $1, 2, \ldots, \frac{1}{2}(p-1)$ are given to a in the series (C) and (E), the (p^2-1) solutions of $z^{p^2-1} \equiv 1$ are obtained in sets of $(p+1)$.

It may be noticed that $aj\epsilon$ has for norm $-a^2b$, and is a solution of $z^{p+1} \equiv -a^2b$; therefore, if a is chosen so that $-a^2b$ is a primitive root of $z^{p-1} \equiv 1$, then $a\epsilon j$ is a primitive root of $z^{p^2-1} \equiv 1$. For

$$(a\epsilon j)^{p+1} \equiv -a^2b \equiv g, \quad \text{and} \quad (a\epsilon j)^{p^2-1} \equiv g^{p-1} \equiv 1.$$

If $p = 4n+3$, the series (A) contains $\pm i$, and the series (B) and (C) are identical with (D) and (E). It is convenient in this case to take the solutions of the congruence $z^{2(p+1)} \equiv 1$. A root of this congruence is $(c+i)(c^2+1)^{-\frac{1}{2}}$, where c is an integer. If η be a primitive root of the congruence, the series

$$1,\ \eta,\ \eta^2,\ \ldots,\ \eta^{2p+1}$$

gives $2(p+1)$ numbers of the class $x+yi$, whose norms are positive or negative unity.

A primitive root of $z^{p^2-1} \equiv 1$ is $a\eta$, where $a^2 \equiv -g$. For

$$(a\eta)^{p+1} \equiv a^2\eta^{p+1} \equiv -a^2 \equiv g \quad \text{and} \quad (a\eta)^{p^2-1} \equiv g^{p-1} \equiv 1.$$

Primitive roots of the congruence $z^{p^2-1} \equiv 1$, mod p, have been found in this way for values of p less than 100, and the series of residues of successive powers have been calculated. Owing to the length of the full tables, only the first $(p+1)$ powers of the selected primitive roots have been given; the other powers may be obtained readily by the numerical cycles of powers of real primitive roots appended in each case.

Thus, if the complete system of 48 residues of the powers of the complex primitive roots in the case of $p = 7$ be written in a matrix of $(p-1)$ rows and $(p+1)$ columns, it is found to consist of the following:—

$$\begin{array}{rrrrrrrr}
3+i, & 1-i, & -3-2i, & -2i, & 2+i, & -2-2i, & 3-i, & 3, \\
2+3i, & 3-3i, & -2+i, & i, & -1+3i, & 1+i, & 2-3i, & 2, \\
-1+2i, & 2-2i, & 1+3i, & 3i, & -3+2i, & 3+3i, & -1-2i, & -1, \\
-3-i, & -1+i, & 3+2i, & 2i, & -2-i, & 2+2i, & -3+i, & -3, \\
-2-3i, & -3+3i, & 2-i, & -i, & 1-3i, & -1-i, & -2+3i, & -2, \\
1-2i, & -2+2i, & -1-3i, & -3i, & 3-2i, & -3-3i, & 1+2i, & 1.
\end{array}$$

The cycle which forms the $(p+1)$-th column, viz.,

$$3,\ 2,\ -1,\ -3,\ -2,\ 1,$$

is a cycle by means of which, given the first row, all the others may be written down by making the x's and y's of the typical term $x+yi$ take in succession the different values in the cycle.

If $x+yj$ is a number, $x-yj$ is its conjugate. Let

$$x+yj = G^m;$$

then

$$x-yj = G^{mp};$$

for it has been shown above that

$$(x+yj)^p \equiv x-yj.$$

It follows that a number and its conjugate are both quadratic residues, or both quadratic non-residues; further, a number is a quadratic residue if its norm is a residue, *i.e.*,

$$\left(\frac{x+yj}{p}\right)_1 = \pm 1,$$

according as

$$\left(\frac{N(x+yj)}{p}\right) = \pm 1.$$

2. *Solution of* $z^{p^n-1}\equiv 1$; $p\equiv 1$, mod n.—The above method may be extended to the solution of $z^{p^n-1}\equiv 1$, mod p, when $p\equiv 1$, mod n.

Here let ω be a primitive root of the equation $x^n-1=0$; there are $(p-1)/n$ non-congruent integers, which are solutions of $y^{(p-1)/n}\equiv 1$, and the same number of solutions of each of the congruences

$$y^{(p-1)/n}\equiv \omega,\ \omega^2,\ \dots,\ \omega^{n-1}.$$

Let a be a solution of $y^{(p-1)/n}\equiv \omega$.

Then $a^{p/n}\equiv \omega a^{1/n}$,

$$a^{p^2/n}\equiv \omega^p a^{p/n}\equiv \omega\,.\,\omega a^{p/n}\equiv \omega^2 a^{1/n}.$$

Proceeding thus, it is established that

$$a^{p^n/n}\equiv \omega^n a^{1/n}\equiv a^{1/n}.$$

Hence $a^{1/n}$ is a solution of the congruence $z^{p^n-1}\equiv 1$, and $a^{2/n}$, $a^{3/n}$, ..., $a^{(n-1)/n}$ are also solutions.

The general solution of the congruence is

$$x_0+x_1a^{1/n}+x_2a^{2/n}+\dots+x_{n-1}a^{(n-1)/n}.$$

By giving to $x_0, x_1, \dots, x_{n-1}$ the integral values less than p, the (p^n-1) solutions of the congruence are found, provided that the value zero is not given to all the x's at the same time.

Particular case; solution of $z^{p^3-1}\equiv 1$, mod p; $p\equiv 1$, mod 3.—Here the general solution is

$$z_0\equiv x_0+x_1a^{\frac{1}{3}}+x_2a^{\frac{2}{3}},$$

$$z_1=z^p\equiv x_0+\omega x_1a^{\frac{1}{3}}+\omega^2x_2a^{\frac{2}{3}},$$

$$z_2=z^{p^2}\equiv x_0+\omega^2x_1a^{\frac{1}{3}}+\omega x_2a^{\frac{2}{3}}.$$

The irreducible factor of the third degree is

$$(z-z_0)(z-z_1)(z-z_2)$$

$$=z^3-3x_0z^2+3\,(x_0^2-ax_1x_2)\,z-x_0^3-ax_1^3-a^2x_2^3+3ax_0x_1x_2.$$

For the primes of the first hundred the primitive roots of the congruence $z^{p^3-1}\equiv 1$ have been computed, and are given in a Table below.

The method of finding the primitive roots closely follows that of the previous case; a primitive root of $z^{p^2+p+1}\equiv 1$ is first determined, the trial values of x_0, x_1, x_2 being connected by the relation

$$x_0^3+ax_1^3+a^2x_2^3-3ax_0x_1x_2\equiv 1.$$

After finding such primitive root ϵ, the required primitive root is given by $g^{\frac{1}{3}}\epsilon$, where g is a primitive root of p. For

$$(g^{\frac{1}{3}}\epsilon)^{p^2+p+1} \equiv g^{\frac{1}{3}(p^2+p+1)} \equiv g^{\frac{1}{3}(p-1)^2+(p-1)+1} \equiv g.$$

Therefore $g^{\frac{1}{3}}\epsilon$ appertains to the index (p^3-1).

3. *Solution of* $z^{p^n-1} \equiv 1$; $p \equiv -1$, mod n.—Case 1. Let n be odd and let γ_1 be a primitive root of the congruence $z^{p^2-1} \equiv 1$, and γ_2 be its conjugate.

Then $$\gamma_1^p \equiv \gamma_2.$$

If ω be a primitive n-th root of unity,

$$\gamma_1^{p/n} \equiv \omega\gamma_2^{1/n}$$

and $$\gamma_2^{p/n} \equiv \omega^{-1}\gamma_1^{1/n}.$$

Hence $$\gamma_1^{p^2/n} \equiv \omega^p\gamma_2^{p/n} \equiv \omega^{-2}\gamma_1^{1/n},$$

$$\gamma_1^{p^3/n} \equiv \omega^3\gamma_2^{1/n}.$$

Since n is odd, $$\gamma_1^{p^n/n} \equiv \omega^n\gamma_2^{1/n} \equiv \gamma_2^{1/n}.$$

Also $$(\gamma_1^{1/n}+\gamma_2^{1/n})^{p^n} \equiv \gamma_1^{p^n/n}+\gamma_2^{p^n/n} \equiv \gamma_2^{1/n}+\gamma_1^{1/n},$$

or $\gamma_1^{1/n}+\gamma_2^{1/n}$ is a solution of $z^{p^n-1} \equiv 1$.

Similarly, $\gamma_1^{2/n}+\gamma_2^{2/n}$, $\gamma_1^{3/n}+\gamma_2^{3/n}$, ... are solutions. The general solution is

$$x_0+x_1(\gamma_1^{1/n}+\gamma_2^{1/n})+x_2(\gamma_1^{2/n}+\gamma_2^{2/n})+\ldots+x_{n-1}(\gamma_1^{(n-1)/n}+\gamma_2^{(n-1)/n}),$$

where the x's may have any integral values.

Case 2. Let n be even, and for simplicity consider $n = 2n_1$, where n_1 is odd. As before, let γ_1 be a primitive root of $z^{p^{n_1}-1} \equiv 1$.

Then $$(\gamma_1^{1/n_1})^{p^{n_1}} \equiv \gamma^{1/n_1}$$

and $$\{(a+bj)\,\gamma_1^{1/n_1}\}^{p^{n_1}} \equiv (a-bj)\,\gamma_2^{1/n_1}.$$

It follows that

$$\{(a+bj)\,\gamma_1^{1/n_1}\}^{p^{2n_1}} \equiv \{(a-bj)\,\gamma_2^{1/n_1}\}^{p^{n_1}} \equiv (a+bj)\,\gamma_1^{1/n_1}.$$

The solution of the congruence $z^{p^n-1} \equiv 1$ is

$$\Sigma\,(x_r+y_rj)\,\gamma_1^{r/n_1},$$

where r has all values from 0 to n_1-1.

The extension to the most general value of n is effected by a similar method; for, if $n = m \, . \, n_1$, where m is a power of 2 and n_1 is odd, the solution of $z^{p^n-1} \equiv 1$ is

$$\Sigma \left(x_{0,r} + x_{1,r} \dot{j}_m + x_{2,r} \dot{j}_m^2 + \ldots + x_{m-1,r} \dot{j}_m^{m-1} \right) \gamma_1^{r/n_1},$$

where the x's are integers, r has all values from 0 to $n_1 - 1$, and the j's are defined thus,

$$\dot{j}_k = \dot{j}_{k+1}^2, \quad \dot{j}_1 = \dot{j}.$$

Particular case; solution of $z^{p^3-1} \equiv 1$, mod p; $p \equiv 2$, mod 3.—The solution in this case is

$$z = x_0 + x_1 (\gamma_1^{\frac{1}{3}} + \gamma_2^{\frac{1}{3}}) + x_2 (\gamma_1^{\frac{2}{3}} + \gamma_2^{\frac{2}{3}}) \; ;$$

whence
$$z^p \equiv x_0 + x_1 (\omega^2 \gamma_1^{\frac{1}{3}} + \omega \gamma_2^{\frac{1}{3}}) + x_2 (\omega \gamma_1^{\frac{2}{3}} + \omega^2 \gamma_2^{\frac{2}{3}}),$$

$$z^{p^2} \equiv x_0 + x_1 (\omega \gamma_1^{\frac{1}{3}} + \omega^2 \gamma_2^{\frac{1}{3}}) + x_2 (\omega^2 \gamma_1^{\frac{2}{3}} + \omega \gamma_2^{\frac{2}{3}}).$$

Hence

$$z^{p^2+p+1} \equiv x_0^3 + x_1^3 (\gamma_1 + \gamma_2) + x_2^3 (\gamma_1^2 + \gamma_2^2) + 6 x_1^2 x_2 (\gamma_1 \gamma_2)^{\frac{2}{3}} + 6 x_1 x_2^2 (\gamma_1 + \gamma_2)(\gamma_1 \gamma_2)^{\frac{1}{3}}$$
$$- 3 x_0 \left\{ x_1^2 (\gamma_1 \gamma_2)^{\frac{1}{3}} + x_1 x_2 (\gamma_1 + \gamma_2) + x_2^2 (\gamma_1 \gamma_2)^{\frac{2}{3}} \right\}.$$

The primitive roots of $z^{p^3-1} \equiv 1$ have been calculated for values of p in the first hundred; these have been effected by guessing $x_0 = 0 = x_2$, in which case

$$z^{p^2+p+1} \equiv x_1^3 (\gamma_1 + \gamma_2),$$

and by assigning a suitable value of x_1, so that the (p^2+p+1)-th power of z shall be a primitive root of p. Further, the powers of z whose indices are factors of (p^2+p+1) have to be examined, and the trial quantities rejected when any of these sub-powers prove congruent to an integer; the examination of these sub-powers was performed by writing

$$z^3 \equiv x_1^3 (\gamma_1 + \gamma_2) + 3 x_1 (\gamma_1 \gamma_2)^{\frac{1}{3}} z,$$

and forming the successive powers of z.

4. *Solution of* $z^{p^n-1} \equiv 1$, $p = nk + q$ *and* $q^2 \equiv 1$, mod n, *n being odd.* Let $n = n_1 n_2$, where n_1 and n_2 are prime to each other, and suppose that

$$q \equiv 1, \text{ mod } n_1, \quad \text{and} \quad \equiv -1, \text{ mod } n_2.$$

Take α a primitive solution of $y^{(p-1)/n_1} \equiv \omega$, and γ_1 a primitive solution of $z^{p^2-1} \equiv 1$, mod p. Then

$$z = a^{t/n_1}(\gamma_1^{t'/n_2} + \gamma_2^{t'/n_2})$$

is a solution of $z^{p^n-1} \equiv 1$. The general solution is

$$z = \Sigma x_{t,t'}\, a^{t/n_1}(\gamma_1^{t/n_2} + \gamma_2^{t'/n_2}),$$

where t is summed from 0 to n_1-1, and t' from 0 to n_2-1, and $x_{t,t'}$ may have any integral value from 0 to $p-1$; by giving all possible values to the x's all the roots are obtained.

In the previous sections the solution of the congruence

$$z^{p^n-1} \equiv 1, \ \text{mod}\ p,$$

has been obtained in the cases in which p or p^2 is congruent to unity, the modulus being n; the solution is expressed in terms of such surd symbols as $\sqrt[n]{a}$ or $\sqrt[n]{\gamma_1}$ and $\sqrt[n]{\gamma_2}$, where a is obtained from Jacobi's tables of residues, and γ_1, γ_2 can be found from the tables given below for primes in the first hundred.

5. It remains to indicate the extension of the method to the general case in which the solution of $z^{p^n-1} \equiv 1$ depends upon that of $z^{p^r} \equiv 1$, where $p^r \equiv 1$, mod n, and $r<n$, but >2.

Let r be the least index for which $p^r \equiv 1$, mod n, and let R_0 be a primitive solution of $z^{p^r-1} \equiv 1$; also represent the conjugate values of R_0 by the symbols $R_1, R_2, \ldots, R_{r-1}$, where

$$R_1 \equiv R_0^p, \quad R_2 \equiv R_0^{p^2}, \quad \ldots, \quad R_{r-1} \equiv R_0^{p^{r-1}}.$$

In the first case, let n be odd, and $p \equiv q$, mod n; also let ω be a primitive n-th root of unity. Then

$$R_0^p \equiv R_1, \quad R_1^p \equiv R_2, \quad \ldots, \quad R_{r-1}^p \equiv R_0.$$

Extracting the n-th roots, we can assign such values to

$$R_0^{1/n}, \quad R_1^{1/n}, \quad \ldots, \quad R_{r-1}^{1/n}$$

that $R_0^{p/n} \equiv \omega R_1^{1/n}$, $R_1^{p/n} \equiv \omega^q R_2^{1/n}$, $R_2^{p/n} \equiv \omega^{q^2} R^{1/n}$, ..., $R_{r-1}^{p/n} \equiv \omega^{q^{r-1}} R_0^{1/n}$.

From these it follows that

$$R_0^{p^2/n} \equiv \omega^p R_1^{p/n} \equiv \omega^{2q} R_2^{1/n},$$

$$R_0^{p^3/n} \equiv \omega^{3q^2} R_3^{1/n}$$

and so on. And, finally,

$$R_0^{p^n/n} \equiv \omega^{nq^{n-1}} R_n^{1/n} \equiv R_n^{1/n}.$$

If n and r have a common factor k, let $n = sk$, $r = s'k$; then

$$\begin{aligned}\left[R_0^{t/n} + R_k^{t/n} + \ldots + R_{(s'-1)k}^{t/n}\right]^{p^n} &\equiv \left[R_0^{p^n t/n} + R_k^{p^n t/n} + \ldots + R_{(s'-1)k}^{p^n t/n}\right] \\ &\equiv R_{sk}^{t/n} + R_{(s+1)k}^{t/n} + \ldots + R_{(s'-1)k}^{t/n} \\ &\equiv R_0^{t/n} + R_k^{t/n} + \ldots + R_{(s'-1)k}^{t/n}.\end{aligned}$$

The solution of $z^{p^n-1} \equiv 1$ is

$$z = \Sigma x_t \left[R_0^{t/n} + R_k^{t/n} + \ldots + R_{(s'-1)k}^{t/n}\right].$$

If r is a factor of n, $s = 1$, and the solution assumes its simplest form; if $k = 1$, n and r are prime and the solution requires all the symbols $R_0^{1/n}, R_1^{1/n}, \ldots, R_{r-1}^{1/n}$.

In certain cases in which $n = n_1 n_2$ and p appertains to an index, modulus n_1, which is a factor of the index to which p appertains when the modulus is n_2, the solution can be written in a somewhat simpler form as in a case considered above.

In the case in which $n = mn$, and $m = 2^k$, the solution is

$$z = \Sigma x_t' \left[R_0^{t/n_1} + R_k^{t/n_1} + \ldots + R_{(s'-1)k}^{t/n_1}\right],$$

where $$x_t' = x_{0,t} + x_{1,t} j_m + x_{2,t} j_m^2 + \ldots + x_{m-1,t} j_m^{m-1},$$

and $$j_k = j_{k+1}^2 \quad \text{and} \quad j_1 = j.$$

TABLE OF RESIDUES OF A PRIMITIVE ROOT OF THE CONGRUENCE $z^{p^2-1} \equiv 1$, mod p. (See p. 297.)

p	
3.	$1+i,\ -i,\ 1-i,\ -1.$ $-1,\ 1.$
5.	$-1-2\sqrt{2},\ -1-\sqrt{2},\ -2\sqrt{2},\ -2+2\sqrt{2},\ -1+2\sqrt{2},\ -2.$ $-2,\ -1,\ 2,\ 1.$
7.	$3+i,\ 1-i,\ -3-2i,\ -2i,\ 2+i,\ -2-2i,\ 3-i,\ 3.$ $3,\ 2,\ -1,\ -3,\ -2,\ 1.$

11. $3-2i,\ 5-i,\ 2-2i,\ 2+i,\ -3-i,\ 3i,\ -5-2i,\ 3+4i,\ -5-5i,\ -3-5i,\ 3+2i,\ 2.$

$2,\ 4,\ -3,\ 5,\ -1,\ -2,\ -4,\ 3,\ -5,\ 1.$

---

13. $4+3\sqrt{2},\ -5-2\sqrt{2},\ -6+3\sqrt{2},\ -6-6\sqrt{2},\ 5-3\sqrt{2},\ 2+3\sqrt{2},\ 5\sqrt{2},$
$4-6\sqrt{2},\ 6+\sqrt{2},\ 4-4\sqrt{2},\ 5-4\sqrt{2},\ -4-\sqrt{2},\ 4-3\sqrt{2},\ -2.$

$-2,\ 4,\ 5,\ 3,\ -6,\ -1,\ 2,\ -4,\ -5,\ -3,\ 6,\ 1.$

---

17. $3+2\sqrt{3},\ 4-5\sqrt{3},\ -1-7\sqrt{3},\ 6-6\sqrt{3},\ -1-6\sqrt{3},\ -5-3\sqrt{3},$
$1-2\sqrt{3},\ 8-4\sqrt{3},\ 4\sqrt{3},\ 7-5\sqrt{3},\ 8-\sqrt{3},\ 1-4\sqrt{3},$
$-4+7\sqrt{3},\ -4-4\sqrt{3},\ -2-3\sqrt{3},\ -7+4\sqrt{3},\ 3-2\sqrt{3},\ -3.$

$-3,\ -8,\ 7,\ -4,\ -5,\ -2,\ 6,\ -1,\ 3,\ 8,\ -7,\ 4,\ 5,\ 2,\ -6,\ 1.$

---

19. $3-i,\ 8-6i,\ -1-7i,\ 9-i,\ 7+7i,\ 9-5i,\ 3-5i,\ 4+i,\ -6-i,$
$3i,\ 3+9i,\ -1+5i,\ 2-3i,\ 3+8i,\ -2+2i,\ -4+8i,\ -4+9i,\ -3-7i,$
$3+i,\ -9.$

$-9,\ 5,\ -7,\ 6,\ 3,\ -8,\ -4,\ -2,\ -1,\ 9,\ -5,\ 7,\ -6,\ -3,\ 8,\ 4,\ 2,\ 1.$

---

23. $-5-10i,\ -6+8i,\ -5-3i,\ -5-4i,\ 8+i,\ -7+7i,\ -10-11i,\ 9-6i,$
$10+9i,\ -6-7i,\ 6+3i,\ -6i,\ 9+7i,\ 2-10i,\ 5+7i,\ -1+7i,$
$6-2i,\ -4-4i,\ 3-9i,\ 10-8i,\ 8+9i,\ 4-10i,\ -5+10i,\ 10.$

$10,\ 8,\ 11,\ -5,\ -4,\ 6,\ -9,\ 2,\ -3,\ -7,\ -1,\ -10,\ -8,\ -11,\ 5,\ 4,\ -6,\ 9,\ -2,$
$3,\ 7,\ 1.$

---

29. $8-2\sqrt{2},\ 14-3\sqrt{2},\ 8+6\sqrt{2},\ 11+3\sqrt{2},\ -11+2\sqrt{2},$
$-9+9\sqrt{2},\ 8+3\sqrt{2},\ -6+8\sqrt{2},\ 7-11\sqrt{2},\ 13+14\sqrt{2},$
$-10-\sqrt{2},\ 11+12\sqrt{2},\ 11-13\sqrt{2},\ -5-10\sqrt{2},\ -12\sqrt{2},$
$-10-9\sqrt{2},\ 14+6\sqrt{2},\ 1-9\sqrt{2},\ -14+13\sqrt{2},\ 10-13\sqrt{2},$
$-13-8\sqrt{2},\ -14-9\sqrt{2},\ 11+14\sqrt{2},\ 3+3\sqrt{2},\ 12-11\sqrt{2},$
$-5+4\sqrt{2},\ 2+13\sqrt{2},\ -7+13\sqrt{2},\ 8+2\sqrt{2},\ -2.$

$-2,\ 4,\ -8,\ -13,\ -3,\ 6,\ -12,\ -5,\ 10,\ 9,\ 11,\ 7,\ -14,\ -1,\ 2,\ -4,\ 8,\ 13,\ 3,$
$-6,\ 12,\ 5,\ -10,\ -9,\ -11,\ -7,\ 14,\ 1.$

---

31. $-3+15i,\ 1+3i,\ 14+6i,\ -8+6i,\ -4-14i,\ 5+13i,\ 7+5i,$
$-3-3i,\ -8-5i,\ 6-12i,\ 7+2i,\ 11+6i,\ 1-8i,\ -7+8i,$
$-6-5i,\ -13i,\ 9+8i,\ 8-13i,\ -15+4i,\ -15+11i,\ 4-10i,$
$14-3i,\ 3+2i,\ -8+8i,\ -3+11i,\ -1+15i,\ -5+2i,\ -15+12i,$
$-11-13i\ \ 11-2i,\ -3-15i,\ -14.$

$-14,\ 10,\ 15,\ 7,\ -5,\ 8,\ 12,\ -13,\ -4,\ -6,\ -9,\ 2,\ 3,\ -11\ \ -1,\ 14,\ -10,$
$-15,\ -7,\ 5,\ -8,\ -12,\ 13,\ 4,\ 9,\ -2,\ -3,\ 11,\ 1.$

37. 8−12√2, −18− 7√2, −13+12√2, 15− 7√2, − 8−14√2,
13−16√2, 7+12√2, −10+12√2, 2− 6√2, 12+ 2√2,
11−17√2, 15− 9√2, 3+ 7√2, 4−17√2, − 4+ √2,
18−18√2, −16+10√2, 2+13√2, 6√2, 4+11√2,
−10+ 3√2, − 4− 4√2, −10+16√2, 17−11√2, − 7+ 4√2,
− 4+ 5√2, − 4+14√2, 2+12√2, −13− 2√2, 18− 8√2,
3+16√2, 10+18√2, 18−13√2, 12+13√2, 6− 3√2,
9+15√2, 8+12√2, − 2.

−2, 4, −8, 16, 5, −10, −17, −3, 6, −12, −13, −11, −15, −7, 14, 9, −18, −1, 2, −4, 8, −16, −5, 10, 17, 3, −6, 12, 13, 11, 15, 7, −14, −9, 18, 1.

---

41. 12+ 5√6, 7− 3√6, − 6− √6, −20− √6, 17+11√6,
1+12√6, 3−15√6, − 4− √6, 4+ 9√6, −10+ 5√6,
−11+10√6, 4−17√6, −11−20√6, 6− 8√6, − 4+16√6,
−19+ 8√6, 12+ √6, 10−10√6, −16+12√6, 4−18√6,
9√6, −17−15√6, 2−19√6, −13−13√6, −13−16√6,
20−11√6, − 8+ 9√6, 10−14√6, −13+ 5√6, − 6− 5√6,
−17− 8√6, 7−17√6, −16− 5√6, −14−17√6, 19+13√6,
3+ 5√6, −19−7 √6, 13−15√6, − 7+ 8√6, − 8+20√6,
12− 5√6, − 6.

−6, −5, −11, −16, 14, −2, 12, 10, −19, −9, 13, 4, 17, −20, −3, 18, 15, −8, 7, −1, 6, 5, 11, 16, −14, 2, −12, −10, 19, 9, −13, −4, −17, 20, 3, −18, −15, 8, −7, 1.

---

43. −19−21i, 6−19i, 3+20i, 19−13i, 11+20i,
− 4− 9i, 16− 3i, 20−21i, − 4−21i, −21+10i,
7− 7i, 21−14i, − 5− 3i, −11−10i, − 1− 9i,
2+20i, − 5+ 8i, 5− 4i, − 7+14i, − 3+10i,
9+ 2i, −12i, 6+13i, −13+14i, −18+ 7i,
16−13i, −18− 3i, 21+ 5i, 7−20i, 6+18i,
6+ 5i, − 9− 6i, 2+ 2i, 4+ 6i, 7+17i,
9+ 3i, 21+12i, −18+19i, 10+17i, − 5−17i,
− 4− 2i, − 9− 7i, −19+21i, −15.

−15, 10, −21, 14, 5, 11, 7, −19, −16, −18, 12, −8, −9, 6, −4, 17, 3, −2, −13, −20, −1, 15, −10, 21, −14, −5, −11, −7, 19, 16, 18, −12, 8, 9, −6, 4, −17, −3, 2, 13, 20, 1.

---

47. −19+ 5i, 7− 2i, 18−21i, − 2+19i, −10+ 5i,
−23− 4i, −13+ 8i, 19+18i, 19−12i, −19− 6i,
15+19i, − 4− 4i, 2+ 9i, 11−20i, −15+12i,
−10−21i, 13+20i, −18+14i, −10+20i, − 4− 7i,
17+19i, 5+ 6i, 16+ 5i, −15i, −19+ 3i,
17−11i, 14+12i, 3−17i, −19+ 9i, −13+16i,

$-21+7i,\quad -12-3i,\quad 8-3i,\quad 4+3i,\quad 3+10i,$
$-13+13i,\quad -6+17i,\quad -18+23i,\quad -8-10i,\quad 14+9i,$
$18-7i,\quad 22-12i,\quad 18+9i,\quad -11+13i,\quad 3-20i,$
$-4+19i,\quad -19-5i,\quad 10.$

10, 6, 13, −11, −16, −19, −2, −20, −12, 21, 22, −15, −9, 4, −7, −23, 5, 3, −17, 18, −8, 14, −1, −10, −6, −13, 11, 16, 19, 2, 20, 12, −21, −22, 15, 9, −4, 7, 23, −5, −3, 17, −18, 8, −14, 1.

53.
$4+3\sqrt{2},\quad -19+24\sqrt{2},\quad 15-14\sqrt{2},\quad -24-11\sqrt{2},\quad -3-10\sqrt{2},$
$-19+4\sqrt{2},\quad 1+12\sqrt{2},\quad 23-2\sqrt{2},\quad -26+8\sqrt{2},\quad -3+7\sqrt{2},$
$-23+19\sqrt{2},\quad 22+7\sqrt{2},\quad 24-12\sqrt{2},\quad 24+24\sqrt{2},\quad -25+9\sqrt{2},$
$7+14\sqrt{2},\quad 6+24\sqrt{2},\quad 9+8\sqrt{2},\quad -22+6\sqrt{2},\quad 1+11\sqrt{2},$
$17-6\sqrt{2},\quad -21-26\sqrt{2},\quad 25-8\sqrt{2},\quad -1-10\sqrt{2},\quad -11+10\sqrt{2},$
$16+7\sqrt{2},\quad 23\sqrt{2},\quad -21-14\sqrt{2},\quad -9-13\sqrt{2},\quad -8-26\sqrt{2},$
$24-22\sqrt{2},\quad 17-16\sqrt{2},\quad 25-13\sqrt{2},\quad 22+23\sqrt{2},\quad 14-\sqrt{2},$
$-3-15\sqrt{2},\quad 4-16\sqrt{2},\quad 26+\sqrt{2},\quad 4-24\sqrt{2},\quad -22+22\sqrt{2},$
$-9+22\sqrt{2},\quad -10+8\sqrt{2},\quad 8+2\sqrt{2},\quad -9-21\sqrt{2},\quad -3-5\sqrt{2},$
$11+24\sqrt{2},\quad -24+23\sqrt{2},\quad -11+20\sqrt{2},\quad 23-6\sqrt{2},\quad 8-8\sqrt{2},$
$17-23\sqrt{2},\quad -17+12\sqrt{2},\quad 4-3\sqrt{2},\quad -2.$

−2, 4, −8, 16, 21, 11, −22, −9, 18, 17, 19, 15, 23, 7, −14, −25, −3, 6, −12, 24, 5, −10, 20, 13, −26, −1, 2, −4, 8, −16, −21, −11, 22, 9, −18, −17, −19, −15, −23, −7, 14, 25, 3, −6, 12, −24, −5, 10, −20, −13, 26, 1.

59.
$4-17i,\quad 22-18i,\quad 18+26i,\quad -17-25i,\quad -21+12i,\quad 2-8i,$
$-10-7i,\quad 18+24i,\quad 8+26i,\quad 2+27i,\quad -5+15i,\quad -1+27i,$
$-17+7i,\quad -8+22i,\quad -12-12i,\quad -16-21i,\quad -8+11i,\quad -22+3i,$
$22-27i,\quad -17-10i,\quad -2+13i,\quad -23+27i,\quad 13+27i,\quad -20+5i,$
$5+6i,\quad 4-2i,\quad -18-17i,\quad -7+2i,\quad 6+9i,\quad -7i,$
$-1-28i,\quad -8+23i,\quad 5-8i,\quad 2+i,\quad 25+29i,\quad 3-14i,$
$10+11i,\quad -9-8i,\quad 5+3i,\quad 12-14i,\quad -13-24i,\quad 12+7i,$
$-10+i,\quad -23-3i,\quad -25+25i,\quad -29-6i,\quad 18-3i,\quad 21-23i,$
$-12+23i,\quad -11+i,\quad -27+14i,\quad 12-16i,\quad 12+27i,\quad -24+22i,$
$-17+24i,\quad -14-28i,\quad -1+8i,\quad 14-10i,\quad 4+17i,\quad 10.$

10, −18, −3, 29, −5, 9, −28, 15, −27, 25, 14, 22, −16, 17, −7, −11, 8, 21, −26, −24, −4, 19, 13, 12, 2, 20, 23, −6, −1, −10, 18, 3, −29, 5, −9, 28, −15, 27, −25, −14, −22, 16, −17, 7, 11, −8, −21, 26, 24, 4, −19, −13, −2, −20, −12, −23, 6, 1.

61.
$2+8\sqrt{2},\quad 10-29\sqrt{2},\quad -17+22\sqrt{2},\quad 13+30\sqrt{2},\quad 18-19\sqrt{2},$
$-24-16\sqrt{2},\quad 1+20\sqrt{2},\quad 17-13\sqrt{2},\quad 9-12\sqrt{2},\quad 9-13\sqrt{2},$
$-7-15\sqrt{2},\quad -10-25\sqrt{2},\quad 7-8\sqrt{2},\quad 8-21\sqrt{2},\quad -15+22\sqrt{2},$
$17-15\sqrt{2},\quad -23-16\sqrt{2},\quad 3+28\sqrt{2},\quad 27+19\sqrt{2},\quad -8+10\sqrt{2},$

$22+17\sqrt{2},\quad 11+27\sqrt{2},\quad 27+20\sqrt{2},\quad 8+12\sqrt{2},\quad 25+27\sqrt{2},$
$-6+10\sqrt{2},\quad 26-28\sqrt{2},\quad -30+30\sqrt{2},\quad -7+3\sqrt{2},\quad -27+11\sqrt{2},$
$-11\sqrt{2},\quad 7-22\sqrt{2},\quad 28+12\sqrt{2},\quad 4+4\sqrt{2},\quad 11-21\sqrt{2},$
$-9-15\sqrt{2},\quad -14+20\sqrt{2},\quad -13-11\sqrt{2},\quad -19-4\sqrt{2},\quad 20+23\sqrt{2},$
$-19+23\sqrt{2},\quad 25+16\sqrt{2},\quad 1-12\sqrt{2},\quad -7-16\sqrt{2},\quad -26-27\sqrt{2},$
$4-18\sqrt{2},\quad 25-4\sqrt{2},\quad -14+9\sqrt{2},\quad -6+28\sqrt{2},\quad 9+8\sqrt{2},$
$24+27\sqrt{2},\quad -8+2\sqrt{2},\quad 16+\sqrt{2},\quad -13+8\sqrt{2},\quad -20-27\sqrt{2},$
$16+30\sqrt{2},\quad 24+5\sqrt{2},\quad 6+19\sqrt{2},\quad 11+25\sqrt{2},\quad -5+16\sqrt{2},$
$2-8\sqrt{2},\quad -2.$

-2, 4, -8, 16, 29, 3, -6, 12, -24, -13, 26, 9, -18, -25, -11, 22, 17, 27, 7, -14, 28, 5, -10, 20, 21, 19, 23, 15, -30, -1, 2, -4, 8, -16, -29, -3, 6, -12, 24, 13, -26, -9, 18, 25, 11, -22, -17, -27, -7, 14, -28, -5, 10, -20, -21, -19, -23, -15, 30, 1.

---

67. $16-15i,\quad 31-11i,\quad -4+29i,\quad -31-12i,\quad -6+5i,\quad -21-31i,$
$3+20i,\quad 13+7i,\quad -22-16i,\quad 11+7i,\quad 13+14i,\quad 16+29i,$
$21+23i,\quad 11-14i,\quad 33+13i,\quad -14-19i,\quad 27-27i,\quad 27-33i,$
$4+5i,\quad 5+20i,\quad -22-23i,\quad -27+29i,\quad 3-2i,\quad 18-10i,$
$4-28i,\quad -21+28i,\quad 17+26i,\quad -8+27i,\quad 9+16i,\quad -18-13i,$
$-14-5i,\quad -31-4i,\quad -20-i,\quad 16i,\quad -28-12i,\quad -25+27i,$
$5+3i,\quad -9-27i,\quad -13-29i,\quad 27-i,\quad 15-19i,\quad 22+7i,$
$-12-17i,\quad 22-25i,\quad -23+7i,\quad 5-12i,\quad -33+i,\quad 23-25i,$
$-7-8i,\quad -31-23i,\quad 30+30i,\quad -8+30i,\quad -13-3i,\quad 15+13i,$
$33-17i,\quad 5-30i,\quad 32-19i,\quad 26+20i,\quad -21-3i,\quad 21-i,$
$-14+4i,\quad -30+6i,\quad 12+10i,\quad 7-20i,\quad 13-23i,\quad -3-27i,$
$16+15i,\quad 12.$

12, 10, -14, 33, -6, -5, 7, 17, 3, -31, 30, 25, 32, -18, -15, 21, -16, 9, -26, 23, 8, 29, 13, 22, -4, 19, 27, -11, 2, 24, 20, -28, -1, -12, -10, 14, -33, 6, 5, -7, -17, -3, 31, -30, -25, -22, 18, 15, -21, 16, -9, 26, -23, -8, -29, -13, -22, 4, -19, -27, 11, -2, -24, -20, 28, 1.

---

71. $15-11i,\quad 33+25i,\quad -11+12i,\quad -33+17i,\quad -24-21i,\quad -23+20i,$
$17-15i,\quad 19+14i,\quad 13+i,\quad -7+14i,\quad -22+3i,\quad -13+3i,$
$-20-25i,\quad -7-13i,\quad -35+24i,\quad 23+35i,\quad 20-12i,\quad 26+26i,$
$-34+33i,\quad -5+17i,\quad -30+26i,\quad -22+10i,\quad -7-34i,\quad 18-7i,$
$-20-19i,\quad -12+6i,\quad 28+9i,\quad 22-31i,\quad -11+3i,\quad 10+24i,$
$-12-34i,\quad 14-23i,\quad 28-2i,\quad -28+17i,\quad -20-5i,\quad 3i,$
$33-26i,\quad -4+28i,\quad 35-33i,\quad 20-28i,\quad -8-i,\quad 11+2i,$
$-26-20i,\quad 29-14i,\quad -3-32i,\quad 29-21i,\quad -9+5i,\quad -9+32i,$
$4+11i,\quad -32-21i,\quad -1-34i,\quad -34-2i,\quad -35-11i,\quad -7+7i,$
$-28-31i,\quad 20-15i,\quad -7-19i,\quad -30+5i,\quad 31-21i,\quad 21-17i,$
$-14+11i,\quad -18+35i,\quad -27+13i,\quad 22-5i,\quad -9-33i,\quad -1+30i,$
$31+35i,\quad -2-29i,\quad 6+13i,\quad 20-13i,\quad 15+11i,\quad -9.$

-9, 10, -19, 29, 23, 6, 17, -11, 28, 32, -4, -35, 31, 5, 26, -21, -24,
3, -27, 30, 14, 16, -2, 18, -20, -23, 13, 25, -12, -34, 22, 15, 7, 8, -1,
9, -10, 19, -29, -23, -6, -17, 11, -28, -32, 4, 35, -31, -5, -26, 21,
24, -3, 27, -30, -14, -16, 2, -18, 20, 23, -13, -25, 12, 34, -22,
-15, -7, -8, 1.

---

73. $5-15\sqrt{5}$, $-18-4\sqrt{5}$, $-9+31\sqrt{5}$, $-34-2\sqrt{5}$, $-20-11\sqrt{5}$,
$-5+26\sqrt{5}$, $-4-14\sqrt{5}$, $8-10\sqrt{5}$, $-13-24\sqrt{5}$, $-17+2\sqrt{5}$,
$-16-27\sqrt{5}$, $-26+32\sqrt{5}$, $25-34\sqrt{5}$, $-26-34\sqrt{5}$, $11+\sqrt{5}$,
$-20-14\sqrt{5}$, $1+11\sqrt{5}$, $-17-33\sqrt{5}$, $-19+17\sqrt{5}$, $17+5\sqrt{5}$,
$2-11\sqrt{5}$, $32-12\sqrt{5}$, $-35-29\sqrt{5}$, $29+15\sqrt{5}$, $-31+5\sqrt{5}$,
$-19-21\sqrt{5}$, $20+34\sqrt{5}$, $32+16\sqrt{5}$, $-18-35\sqrt{5}$, $-20+22\sqrt{5}$,
$2-28\sqrt{5}$, $-7-24\sqrt{5}$, $13-15\sqrt{6}$, $22+22\sqrt{5}$, $-7-\sqrt{5}$,
$-33+27\sqrt{5}$, $-27\sqrt{5}$, $-19+11\sqrt{5}$, $29-25\sqrt{5}$, $-24+24\sqrt{5}$,
$-22-31\sqrt{5}$, $25+29\sqrt{5}$, $-6-11\sqrt{5}$, $-8+35\sqrt{5}$, $36+3\sqrt{5}$,
$28-14\sqrt{5}$, $22+21\sqrt{5}$, $-5-6\sqrt{5}$, $-13-28\sqrt{5}$, $-9-18\sqrt{5}$,
$-9-28\sqrt{5}$, $11-5\sqrt{5}$, $-8+29\sqrt{5}$, $-25-27\sqrt{5}$, $2+21\sqrt{5}$,
$-32+2\sqrt{5}$, $-18-21\sqrt{5}$, $25+19\sqrt{5}$, $14+12\sqrt{5}$, $-27-4\sqrt{5}$,
$19+20\sqrt{5}$, $-18+34+5$, $-12+2\sqrt{5}$, $9-29\sqrt{5}$, $30+12\sqrt{5}$,
$-20-25\sqrt{5}$, $23+29\sqrt{5}$, $-16+19\sqrt{5}$, $28-30\sqrt{5}$, $-19+14\sqrt{5}$,
$23-10\sqrt{5}$, $-11-30\sqrt{5}$, $5+15\sqrt{5}$, -5.

-5, 25, 21, -32, 14, 3, -15, 2, -10, -23, -31, 9, 28, 6, -30, 4, -20,
27, 11, 18, -17, 12, 13, 8, 33, -19, 22, 36, -34, 24, 26, 16, -7, 35, -29,
-1, 5, -25, -21, 32, -14, -3, 15, -2, 10, 23, 31, -9, -28, -6, 30, -4,
20, -27, -11, -18, 17, -12, -13, -8, -33, 19, -22, -36, 34, -24,
-26, -16, 7, -35, 29, 1.

---

79. $33+21i$, $16-36i$, $20+17i$, $-13+33i$, $-16+26i$, $32-31i$,
$-31-35i$, $28+11i$, $-18+3i$, $-25+37i$, $-22-15i$, $-16-9i$,
$-23-i$, $-27+37i$, $-9+22i$, $31-16i$, $16-35i$, $-1-29i$,
$23-30i$, $-33-33i$, $-1+35i$, $22+28i$, $-20-36i$, $17-28i$,
$-36-14i$, $-25-33i$, $26-34i$, $-8-23i$, $-18+21i$, $-8-i$,
$-6+36i$, $-6+35i$, $15+2i$, $-21-14i$, $-4-34i$, $29-21i$,
$-24-5i$, $24-37i$, $-11-6i$, $-34i$, $3-16i$, $-39+9i$,
$25+31i$, $16-32i$, $15-9i$, $-27+18i$, $-5+27i$, $-21-4i$,
$23-20i$, $-6-19i$, $-36+37i$, $10-9i$, $-34-8i$, $-6-30i$,
$37-10i$, $9-27i$, $-5+9i$, $-38+34i$, $7+8i$, $-16+16i$,
$5+34i$, $4-37i$, $-39-31i$, $-4-25i$, $-2+39i$, $-16-19i$,
$29-15i$, $8+35i$, $3-20i$, $-34+35i$, $39-33i$, $5-33i$,
$-11-36i$, $-2+3i$, $29-22i$, $-3-38i$, $-12+26i$, $6-26i$,
$33-21i$, 29.

29, -28, -22, -6, -16, 10, -26, 36, 17, 19, -2, 21, -23, -35, 12, 32,
-20, -27, 7, -34, -38, 4, 37, -33, -9, -24, 15, -39, -25, -14, -11,
-3, -8, 5, -13, 18, -31, -30, -1, -29, 28, 22, 6, 16, -10, 26, -36,
-17, -19, 2, -21, 23, 35, -12, -32, 20, 27, -7, 34, 38, -4, -37, 33,
9, 24, -15, 39, 25, 14, 11, 3, 8, -5, 13, -18, 31, 30, 1.

83. $38+10i,\quad 16+13i,\quad -20-10i,\quad 4+i,\quad -24-5i,\quad -32-15i,$
$13+23i,\quad 15+8i,\quad -8+39i,\quad -30-9i,\quad 29+22i,\quad -31-36i,$
$12-18i,\quad -28+17i,\quad 11+34i,\quad -5-9i,\quad -17+23i,\quad 37+40i,$
$10-19i,\quad -11-41i,\quad -8-8i,\quad 25+31i,\quad -24+17i,\quad -3-9i,$
$-24-40i,\quad -14-17i,\quad -30-39i,\quad -3-39i,\quad 27-18i,\quad -39+i,$
$2-20i,\quad 27+7i,\quad -40+38i,\quad 9-35i,\quad 28+5i,\quad 18-28i,$
$-32+29i,\quad -12+35i,\quad 24-35i,\quad 17-11i,\quad 9+i,\quad -38i,$
$-35-33i,\quad -4-27i,\quad 35+13i,\quad 38+14i,\quad -24-i,\quad 11-29i,$
$-39+4i,\quad -28+11i,\quad -12-28i,\quad -10-22i,\quad 6-23i,\quad -40+16i,$
$-20-41i,\quad -18-15i,\quad -36-3i,\quad -10+24i,\quad -39-18i,\quad 26+5i,$
$25+35i,\quad 19+3i,\quad 28-28i,\quad 16-37i,\quad -18-i,\quad -10+31i,$
$-26-i,\quad 18+34i,\quad 12-22i,\quad 12+31i,\quad -20-30i,\quad 38-12i,$
$-13+7i,\quad 17-30i,\quad 33+26i,\quad -2-10i,\quad 24+15i,\quad 15-20i,$
$23-29i,\quad 2+41i,\quad -2+i,\quad -3+18i,\quad 38-10i,\quad -33.$

−33, 10, 2, 17, 20, 4, 34, 40, 8, −15, −3, 16, −30, −6, 32, 23, −12, −19, −37, −24, −38, 9, 35, 7, 18, −13, 14, 36, −26, 28, −11, 31, −27, −22, −21, 29, 39, 41, −25, −5, −1, 33, −10, −2, −17, −20, −4, −34, −40, −8, 15, 3, −16, 30, 6, −32, −23, 12, 19, 37, 24, 38, −9, −35, −7, −18, 13, −14, −36, 26, −28, 11, −31, 27, 22, 21, −29, −39, −41, 25, 5, 1.

---

89. $3+2\sqrt{3},\quad 21+12\sqrt{3},\quad -43-11\sqrt{3},\quad -17-30\sqrt{3},\quad 36-35\sqrt{3},$
$-13-33\sqrt{3},\quad 30-36\sqrt{3},\quad -37+41\sqrt{3},\quad -43-40\sqrt{3},\quad -13-28\sqrt{3},$
$-29-21\sqrt{3},\quad -35-32\sqrt{3},\quad -30+12\sqrt{3},\quad -18-24\sqrt{3},\quad -20-19\sqrt{3},$
$4-8\sqrt{3},\quad -36-16\sqrt{3},\quad -26-31\sqrt{3},\quad 3+33\sqrt{3},\quad 29+16\sqrt{3},$
$5+17\sqrt{3},\quad 28-28\sqrt{3},\quad 5-28\sqrt{3},\quad 25+15\sqrt{3},\quad -13+6\sqrt{3},$
$-3-8\sqrt{3},\quad 32-30\sqrt{3},\quad 5-26\sqrt{3},\quad 37+21\sqrt{3},\quad -30-41\sqrt{3},$
$20-5\sqrt{3},\quad 30+25\sqrt{3},\quad -27-43\sqrt{3},\quad 17-5\sqrt{3},\quad 21+19\sqrt{3},$
$-1+10\sqrt{3},\quad -32+28\sqrt{3},\quad -17+20\sqrt{3},\quad -20+26\sqrt{3},\quad 7+38\sqrt{3},$
$-18+39\sqrt{3},\quad 2-8\sqrt{3},\quad -42-20\sqrt{3},\quad 21+34\sqrt{3},\quad -34\sqrt{3},$
$-26-13\sqrt{3},\quad 22-2\sqrt{3},\quad -35+38\sqrt{3},\quad 34+44\sqrt{3},\quad 10+22\sqrt{3},$
$-16-3\sqrt{3},\quad 23-41\sqrt{3},\quad 1+12\sqrt{3},\quad -14+38\sqrt{3},\quad 8-3\sqrt{3},$
$6+7\sqrt{3},\quad -29+33\sqrt{3},\quad 22+41\sqrt{3},\quad -44-11\sqrt{3},\quad -20-32\sqrt{3},$
$15+42\sqrt{3},\quad 30-22\sqrt{3},\quad -42-6\sqrt{3},\quad 16-13\sqrt{3},\quad -30-7\sqrt{3},$
$-43+8\sqrt{3},\quad 8+27\sqrt{3},\quad 8+8\sqrt{3},\quad -17+40\sqrt{3},\quad 11-3\sqrt{3},$
$15+13\sqrt{3},\quad 34-20\sqrt{3},\quad -18+8\sqrt{3},\quad -6-12\sqrt{3},\quad -1+41\sqrt{3},$
$-24+32\sqrt{3},\quad 31-41\sqrt{3},\quad 25+28\sqrt{3},\quad -24-44\sqrt{3},\quad 20-2\sqrt{3},$
$-41+34\sqrt{3},\quad -8+20\sqrt{3},\quad 7+44\sqrt{3},\quad 18-32\sqrt{3},\quad 40+29\sqrt{3},$
$27-11\sqrt{3},\quad 15+21\sqrt{3},\quad -7+4\sqrt{3},\quad 3-2\sqrt{3},\quad -3.$

−3, 9, −27, −8, 24, 17, 38, −25, −14, 42, −37, 22, 23, 20, 29, 2, −6, 18, 35, −16, −41, 34, −18, 39, −28, −5, 15, 44, −43, 40, −31, 4, −12, 36, −19, −32, 7, −21, −26, −11, 33, −10, 30, −1, 3, −9, 27, 8, −24, −17, −38, 25, 14, −42, 37, −22, −23, −20, −29, −2, 6, −18, −35, 16, 41, −34, 18, −39, 28, 5, −15, −44, 43, −40, 31, −4, 12, −36, 19, 32, −7, 21, 26, 11, −33, 10, −30, 1.

97. $-47+4\sqrt{5}$, $-39+12\sqrt{5}$, $36-41\sqrt{5}$, $10+34\sqrt{5}$, $16-6\sqrt{5}$,
$1-42\sqrt{5}$, $-14+38\sqrt{5}$, $-37+\sqrt{5}$, $13-\sqrt{5}$, $48+2\sqrt{5}$,
$15+\sqrt{5}$, $-6+13\sqrt{5}$, $-40+44\sqrt{5}$, $44+3\sqrt{5}$, $29+35\sqrt{5}$,
$16+23\sqrt{5}$, $-1-47\sqrt{5}$, $-20-26\sqrt{5}$, $32-22\sqrt{5}$, $-4-2\sqrt{5}$,
$-46-19\sqrt{5}$, $36+30\sqrt{5}$, $-25-5\sqrt{5}$, $8+38\sqrt{5}$, $-4-8\sqrt{5}$,
$28-28\sqrt{5}$, $-33-27\sqrt{5}$, $41-27\sqrt{5}$, $-42-22\sqrt{5}$, $-18-7\sqrt{5}$,
$27-34\sqrt{5}$, $-9-40\sqrt{5}$, $11+\sqrt{5}$, $-12-3\sqrt{5}$, $19-4\sqrt{5}$,
$-3-27\sqrt{5}$, $-11-4\sqrt{5}$, $-48+47\sqrt{5}$, $-5+24\sqrt{5}$, $36+16\sqrt{5}$,
$-14-26\sqrt{5}$, $41+2\sqrt{5}$, $-44-27\sqrt{5}$, $-24+26\sqrt{5}$, $-1+40\sqrt{5}$,
$-26-41\sqrt{5}$, $14-20\sqrt{5}$, $9+26\sqrt{5}$, $-22\sqrt{5}$, $45-33\sqrt{5}$,
$38-15\sqrt{5}$, $48-16\sqrt{5}$, $43-26\sqrt{5}$, $-19+36\sqrt{5}$, $-36-22\sqrt{5}$,
$-9+17\sqrt{5}$, $-13+38\sqrt{5}$, $13+5\sqrt{5}$, $-26+11\sqrt{5}$, $-13-39\sqrt{5}$,
$25+35\sqrt{5}$, $10+7\sqrt{5}$, $-39+2\sqrt{5}$, $30+41\sqrt{5}$, $-8+36\sqrt{5}$,
$29+22\sqrt{5}$, $47-45\sqrt{5}$, $-5-25\sqrt{5}$, $26-9\sqrt{5}$, $-44+42\sqrt{5}$,
$-2-16\sqrt{5}$, $-32-32\sqrt{5}$, $-9+18\sqrt{5}$, $7-9\sqrt{5}$, $-24-34\sqrt{5}$,
$-37+47\sqrt{5}$, $-37-29\sqrt{5}$, $-5-46\sqrt{5}$, $-6+8\sqrt{5}$, $43-12\sqrt{5}$,
$35+4\sqrt{5}$, $-13-48\sqrt{5}$, $39-27\sqrt{5}$, $-45-30\sqrt{5}$, $-37-31\sqrt{5}$,
$-45+48\sqrt{5}$, $-29-11\sqrt{5}$, $-21+13\sqrt{5}$, $-14-16\sqrt{5}$, $47+17\sqrt{5}$,
$-26-29\sqrt{5}$, $-37-2\sqrt{5}$, $-47+43\sqrt{5}$, $-35+22\sqrt{5}$, $48-10\sqrt{5}$,
$-31-17\sqrt{5}$, $-47-4\sqrt{5}$, -5.

−5, 25, −28, 43, −21, 8, −40, 6, −30, −44, 26, −33, −29, 48, −46, 36, 14, 27, −38, −4, 20, −3, 15, 22, −13, −32, −34, −24, 28, −19, −7, 35, 19, 2. −10, −47, 41, −11, −42, 16, 17, 12, 37, 9, −45, 31, 39, −1, 5, −25, 28, −43, 21, −8, 40, −6, 30, 44, −26, 33, 29, −48, 46, −36, −14, −27, 38, 4, −20, 3, −15, −22, 13, 32, 34, 24, −23, 18, 7, −35, −19, −2, 10, 47, −41, 11, 42, −16, −17, −12, −37, −9, 45, −31, −39, 1.

TABLE OF PRIMITIVE ROOTS OF $z^{p^2-1} \equiv 1$, mod p. (See p. 298.)

p	$\frac{1}{3}(p^2+p+1)$	ϵ	$g^{\frac{1}{3}}$	Primitive Root	Irreducible Factor
7	19	$3+\sqrt[3]{9}$	$\sqrt[3]{3}$	$3+3\sqrt[3]{3}$	z^3-2z^2-z-3
13	61	$-2-\sqrt[3]{4}$	$-\sqrt[3]{2}$	$2+2\sqrt[3]{2}$	z^3-6z^2-z+2
19	127	$5+4\sqrt[3]{4}$	$-4\sqrt[3]{4}$	$6\sqrt[3]{2}-\sqrt[3]{4}$	z^3+2z-8
31	331	$2+2\sqrt[3]{3}$	$8\sqrt[3]{3}$	$-15\sqrt{3}-15\sqrt[3]{9}$	$z^3+8z+14$
37	7 . 67	$9+14\sqrt[3]{2}$	$-\sqrt[3]{2}$	$-9\sqrt[3]{2}-14\sqrt[3]{4}$	$z^3+16z+2$
43	631	$-5-\sqrt[3]{3}$	$3\sqrt[3]{9}$	$-9-15\sqrt[3]{9}$	$z^3-16z^2-16z+15$
61	13 . 97	$-4+\sqrt[3]{4}$	$-\sqrt[3]{2}$	$-2+4\sqrt[3]{2}$	$z^3+6z^2+12z+2$
67	7^2 . 31	$-29+29\sqrt[3]{2}$	$-4\sqrt[3]{4}$	$-31-18\sqrt[3]{4}$	$z^3-26z^2-2z-12$
73	1801	$8+8\sqrt[3]{2}+8\sqrt[3]{4}$	$11\sqrt[3]{4}$	$30+30\sqrt[3]{2}+15\sqrt[3]{4}$	$z^3-19z^2+15z-29$
79	7^2 . 43	$-23+23\sqrt[3]{2}$	$3\sqrt[3]{4}$	$-20+10\sqrt[3]{4}$	z^3+13z^2+5
97	3169	$46-6\sqrt{2}$	$20\sqrt[3]{2}$	$47\sqrt[3]{2}-23\sqrt[3]{4}$	$z^3-20z-44$

TABLE OF PRIMITIVE ROOTS OF $z^{p^3-1} \equiv 1$, mod p—(*continued*).
(See p. 300.)

p	p^2+p+1	z^{p^2+p+1}	Primitive Root	Irreducible Factor
5	31	-2	$(-1-2\sqrt{2})^{\frac{1}{3}}+(-1+2\sqrt{2})^{\frac{1}{3}}$	z^3-z+2
11	7.19	6	$(3-2i)^{\frac{1}{3}}+(3+2i)^{\frac{1}{3}}$	z^3+z+5
17	307	6	$(3-2\sqrt{3})^{\frac{1}{3}}+(3+2\sqrt{3})^{\frac{1}{3}}$	z^3+4z-6
23	7.79	-8	$5\left\{(-5-10i)^{\frac{1}{3}}+(-5+10i)^{\frac{1}{3}}\right\}$	z^3-7z+8
29	13.67	-3	$3\left\{(8-2\sqrt{2})^{\frac{1}{3}}+(8+2\sqrt{2})^{\frac{1}{3}}\right\}$	z^3+6z+3
41	1723	-17	$(12-5\sqrt{6})^{\frac{1}{3}}+(12+5\sqrt{6})^{\frac{1}{3}}$	$z^3-5z+17$
47	37.61	-3	$5\left\{(-19-5i)^{\frac{1}{3}}+(-19+5i)^{\frac{1}{3}}\right\}$	z^3+4z+3
53	7.409	8	$(4-3\sqrt{2})^{\frac{1}{3}}+(4+3\sqrt{2})^{\frac{1}{3}}$	z^3+z-8
59	3541	8	$(4-17i)^{\frac{1}{3}}+(4+17i)^{\frac{1}{3}}$	$z^3+16z-8$
71	5113	-9	$47\left\{(15-11i)^{\frac{1}{3}}+(15+11i)^{\frac{1}{3}}\right\}$	$z^3+12z+9$
83	19.367	-7	$(38-10i)^{\frac{1}{3}}+(38+10i)^{\frac{1}{3}}$	$z^3-18z+7$
89	8011	6	$(3-2\sqrt{3})^{\frac{1}{3}}+(3+2\sqrt{3})^{\frac{1}{3}}$	z^3-2z+6

Thursday, February 14th, 1901.

Dr. HOBSON, F.R.S., President, in the Chair.

Thirteen members present.

The President prefaced the business of the evening with the following remarks upon recent losses :—

"It would not be fitting that we should commence the business of the meeting without some reference being made to the great loss which has been sustained by the nation since our last meeting. It is not for me to dwell upon the great personal qualities of Her late Majesty ; that has been done in ample measure by many others more fitted to do it than I can claim to be. A certain measure of political stability in a country is usually necessary to produce conditions favourable to progress in science ; to the production of such political stability the great personal qualities of the Queen have contributed in large measure. To appreciate this we need only to look back to the time of her immediate predecessors. In the earlier part of the nineteenth century the progress of our science was checked by the reactionary spirit which resulted partly from fear due to the excesses of the French Revolution, and which prevented our utilizing the great progress which had been made in mathematics on the Continent.

"Since our last meeting the death has occurred of the very distinguished French mathematician Charles Hermite. He was our senior foreign member, being the survivor of several distinguished foreign members elected in the year 1872. The importance of his work in the theories of forms and of elliptic functions is recognized by all specialists in those subjects. His work *Sur quelques Applications des Fonctions Elliptiques* has enabled a comparatively wide circle of readers, not all of them pure mathematicians, to appreciate his great analytical power. Not the least of Hermite's achievements was his proof of the transcendency of the number e, the base of Napierian logarithms. His method under the hands of Lindemann led to the proof of the corresponding result for the number π; thus the *coup de grâce* was given to the circle squarer. Hermite was more fortunate than many others in being able to continue his scientific activity into a good old age."

On the motion of the Treasurer a resolution that the President's remarks should be entered upon the minutes was carried unanimously.

Dr. Larmor gave an abstract of a paper by Mr. T. Stuart, entitled "The Distribution of Velocity and the Equations of the Stream Lines due to the Motion of an Ellipsoid in Fluid Frictionless and Viscous."

Lt.-Col. Cunningham communicated a paper "On Factorisable Twin Binomials." Mr. Bickmore also spoke on the subject.

Mr. Tucker gave a short account of a note on "The Brocardal Properties of some Associated Triangles."

The following papers were communicated from the Chair:—

Concerning the Abelian and related Linear Groups: by Dr. L. E. Dickson.

A Geometrical Theory of Differential Equations of the First and Second Orders: by Mr. R. W. H. T. Hudson.

A Note on Stability, with a Hydrodynamical Application: by Mr. Bromwich.

(1) Remarks on Notation in Lie's Theory of Groups; and (2) On Schur's Determination of a Continuous Group of given Structure, with remarks on Mr. Campbell's paper (read at January meeting): by Mr. H. F. Baker.

Note on Curves Similar and Parallel to one another: by Mr. D. B. Mair.

The following presents were made to the Library:—

"Educational Times," February, 1901.

"Indian Engineering," Vol. xxviii., Nos. 25, 26, 1900; Vol. xxix., Nos. 1, 2, 3, Dec. 22, 1900–Jan. 19, 1901.

The following exchanges were received:—

"Proceedings of the Royal Society," Vol. lxvii., Nos. 440, 441; 1901.

"Beiblätter zu den Annalen der Physik und Chemie," Bd. xxiv., St. 12; Bd. xxv., St. 1; Leipzig, 1900–1.

"Rendiconti del Circolo Matematico di Palermo," Tomo xiv., Fasc. 6; 1900.

"Bulletin of the American Mathematical Society," Series 2, Vol. vii., No. 4, January, and "Annual Register"; New York, 1901.

"Bulletin des Sciences Mathématiques," Tome xxiv., Oct.; Paris, 1900.

"Rendiconto dell' Accademia delle Scienze Fisiche e Matematiche," Serie 3, Vol. vi., Fasc. 8–12; Napoli, 1900.

"Journal für die reine und angewandte Mathematik," Band cxxiii., Heft 1; Berlin, 1901.

"Annali di Matematica," Serie 3, Tomo v., Fasc. 2; Milano, 1901.

"Archives Néerlandaises," Série 2, Tome v.; La Haye, 1900.

"Atti della Reale Accademia dei Lincei—Rendiconti," Sem. 2, Vol. ix., Fasc. 12; Sem. 1, Vol. x., Fasc. 1, 2; Roma, 1900, 1901.

"Revue Semestrielle des Publications Mathématiques," Tome ix., Pte. 1, Av.-Oct.; 1900.

"Journal of the Institute of Actuaries," Vol. xxxv., Pt. 6, Jan., 1901.

"Nieuw Archief voor Wiskunde," Reeks 2, Deel v., St. 1; Amsterdam, 1901.

"Wiskundige Opgaven," Deel viii., St. 3; Amsterdam, 1900.

"Sitzungsberichte der Königl. Preuss. Akademie der Wissenschaften zu Berlin," Nos. 39–53, 1900.

"Proceedings of the Cambridge Philosophical Society," Vol. x., Pt. 7; Vol. xi., Pt. 1; "List of Members, &c."; 1901.

"Nachrichten von der Königl. Gesellschaft der Wissenschaften zu Göttingen," Math.-Phys. Kl., Heft 3; Geschäftliche Mitteilungen, Heft 2; 1900.

"Proceedings of the Canadian Institute," Vol. ii., Pt. 4, No. 10; Toronto, 1901.

"Annals of Mathematics," Vol. ii., No. 2; January, 1901.

"Periodico di Matematica," Serie 2, Vol. iii., Fasc. 4; Livorno, 1901.

"Supplemento al Periodico di Matematica," Anno iv., Fasc. 2; Livorno, 1900.

"Proceedings of the American Philosophical Society," Vol. xxxix., No. 163; Philadelphia, 1900.

Concerning the Abelian and related Linear Groups. *By* L. E. Dickson, Ph.D.

Received January 21st, 1901. Communicated February 14th, 1901.

1. The object of the paper is to determine by elementary methods a classification of the substitutions of the special Abelian group of quaternary substitutions modulo 3, $SA\,(4, 3)$, into complete sets of conjugates. When complications are not introduced, the methods are applied to the corresponding group $SA\,(4, p^n)$ in the general Galois field; in particular, its substitutions of periods 2 and 4 are determined (§§ 2–4). The types of substitutions of period 3 in $SA\,(4, 3^n)$ are determined in § 7. In § 9 is exhibited a table of the non-conjugate types of substitutions of the group $SA\,(4, 3)$, and the number of conjugates to each within the group. This group, $SA\,(4, 3)$, is the group for the trisection of the periods of a hyperelliptic function of four periods. The order of $SA\,(4, p^n)$ is

$$p^{4n}(p^{4n}-1)(p^{2n}-1).$$

By a more complicated analysis, depending upon the possible forms of the characteristic determinant of an Abelian substitution, the corresponding problem for $SA\,(4, p^n)$ has been solved by the writer.* In the present paper, on the other hand, the classification is based upon the periods of the substitutions.†

In § 10 is determined the structure of a group whose definition is analogous to that of the Abelian group.

For the substitutions of $SA\,(4, p^n)$ the usual notation is used:

$$\begin{array}{c|cccc|}
 & \xi_1 & \eta_1 & \xi_2 & \eta_2 \\
\hline
\xi_1' = & \alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12} \\
\eta_1' = & \beta_{11} & \delta_{11} & \beta_{12} & \delta_{12} \\
\xi_2' = & \alpha_{21} & \gamma_{21} & \alpha_{22} & \gamma_{22} \\
\eta_2' = & \beta_{21} & \delta_{21} & \beta_{22} & \delta_{22}
\end{array}\,.$$

---

* *Transactions of the American Mathematical Society*, Vol. II., pp. 103–138.

† As a check upon the work, it was found that the results for $p^n = 3$ were the same in the two investigations.

Quaternary Abelian Substitutions of periods 2 *and* 4.

2. Within $SA\,(4, p^n)$, $p > 2$, every substitution of period 2 is conjugate with $T_{1,-1}$ or $T \equiv T_{1,-1}T_{2,-1}$.* Hence a substitution of period 4 is within $SA\,(4, p^n)$ conjugate with S, where $S^2 = T_{1,-1}$, or with S_1, where $S_1^2 = T$. Within $SA\,(4, p^n)$, $p > 2$, S_1 is conjugate with M_1M_2.†

The identity $ST_{1,-1} = S_{-1}$ or

$$\left\{\begin{matrix} -\alpha_{11} & -\gamma_{11} & -\alpha_{12} & -\gamma_{12} \\ -\beta_{11} & -\delta_{11} & -\beta_{12} & -\delta_{12} \\ \alpha_{21} & \gamma_{21} & \alpha_{22} & \gamma_{22} \\ \beta_{21} & \delta_{21} & \beta_{22} & \delta_{22} \end{matrix}\right\} = \left\{\begin{matrix} \delta_{11} & -\gamma_{11} & \delta_{21} & -\gamma_{21} \\ -\beta_{11} & \alpha_{11} & -\beta_{21} & \alpha_{21} \\ \delta_{12} & -\gamma_{12} & \delta_{22} & -\gamma_{22} \\ -\beta_{12} & \alpha_{12} & -\beta_{22} & \alpha_{22} \end{matrix}\right\}$$

requires, for $p > 2$, that S shall have the form

$$\left\{\begin{matrix} \alpha_{11} & \gamma_{11} & 0 & 0 \\ \beta_{11} & -\alpha_{11} & 0 & 0 \\ 0 & 0 & \alpha_{22} & 0 \\ 0 & 0 & 0 & \alpha_{22} \end{matrix}\right\} \qquad (\alpha_{22}^2 = 1).$$

Hence $S = A$ or $AT_{2,-1}$, where A affects only ξ_1 and η_1, while $A^2 = T_{1,-1}$. But A is conjugate with both M_1 and $M_1T_{1,-1}$ by Abelian substitutions affecting only ξ_1, η_1.‡ Hence within $SA\,(4, p^n)$, $p > 2$, S is conjugate either with M_1 or else with $M_1T_{1,-1}T_{2,-1}$, the latter two being not conjugate.

To determine the number of substitutions conjugate with M_1, consider the conditions for the identity $SM_1 = M_1S$. For $p > 2$, S must have the form

$$(1) \quad \left\{\begin{matrix} \alpha_{11} & \gamma_{11} & 0 & 0 \\ -\gamma_{11} & \alpha_{11} & 0 & 0 \\ 0 & 0 & \alpha_{22} & \gamma_{22} \\ 0 & 0 & \beta_{22} & \delta_{22} \end{matrix}\right\}.$$

The Abelian relations require $\alpha_{22}\delta_{22} - \beta_{22}\gamma_{22} = 1$, having $p^n(p^{2n}-1)$ sets of solutions in the $GF[p^n]$, and $\alpha_{11}^2 + \gamma_{11}^2 = 1$, having $p^n - \epsilon$ sets of solutions, $\epsilon = \pm 1$ according as $p^n = 4l \pm 1$. Hence M_1 is one of $p^{3n}(p^{2n}+1)(p^n+\epsilon)$ substitutions conjugate within $SA(4, p^n)$. Evidently $M_1 T_{1,-1} T_{2,-1}$ is one of an equal number of conjugates.

---

* *Proceedings of the London Mathematical Society*, Vol. xxxi., pp. 54–59.

† *Quarterly Journal*, Vol. xxxii., pp. 56–58, § 9.

‡ *Ibid.*, § 8.

3. If $SA(4, p^n)$ contains a substitution S whose square is M_1, then S must be commutative with $M_1 \equiv S^2$, and hence be of the form (1). But $S = S^{-1}M_1$ gives $\alpha_{11} = \gamma_{11}$, $\alpha_{22} = \delta_{22}$, $\beta_{22} = \gamma_{22} = 0$. Hence S exists only when 2 is a square in the $GF[p^n]$, for which case there are four substitutions whose square is M_1.

If $S^2 = M_1 T_{1,-1} T_{2,-1}$, then S must be commutative with M_1, and hence have the form (1). Then $S = S^{-1}M_1 T_{1,-1} T_{2,-1}$ requires $\alpha_{11} = -\gamma_{11}$, $\alpha_{22} = -\delta_{22}$, so that 2 must be a square in the field. The number of substitutions S is double the number of sets of solutions in the field of $-\alpha_{22}^2 - \beta_{22}\gamma_{22} = 1$.

4. The remaining type $M_1 M_2$ is not conjugate with M_1 or $M_1 T$, as their squares are not conjugate. The most general linear substitution commutative with $M_1 M_2$ has the form

$$(2) \quad \left\{\begin{array}{cccc} \alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12} \\ -\gamma_{11} & \alpha_{11} & -\gamma_{12} & \alpha_{12} \\ \alpha_{21} & \gamma_{21} & \alpha_{22} & \gamma_{22} \\ -\gamma_{21} & \alpha_{21} & -\gamma_{22} & \alpha_{22} \end{array}\right\}.$$

The six Abelian conditions reduce to the following four:—

$$(3) \quad \left\{\begin{array}{ll} \alpha_{11}^2+\gamma_{11}^2+\alpha_{12}^2+\gamma_{12}^2 = 1, & \alpha_{11}\gamma_{21}-\gamma_{11}\alpha_{21}+\alpha_{12}\gamma_{22}-\gamma_{12}\alpha_{22} = 0, \\ \alpha_{22}^2+\gamma_{22}^2+\alpha_{21}^2+\gamma_{21}^2 = 1, & \alpha_{11}\alpha_{21}+\gamma_{11}\gamma_{21}+\alpha_{12}\alpha_{22}+\gamma_{12}\gamma_{22} = 0. \end{array}\right.$$

Hence, when (2) is Abelian, it is also orthogonal, and leaves $\xi_1^2+\eta_1^2+\xi_2^2+\eta_2^2$ absolutely invariant. To determine the number of these substitutions, introduce the new indices*

$$X_1 = \xi_1 + i\eta_1, \quad Y_1 = \xi_1 - i\eta_1, \quad X_2 = \xi_2 + i\eta_2, \quad Y_2 = \xi_2 - i\eta_2,$$

where $i^2 = -1$. Then (2) takes the form

$$(4) \quad X_j' = A_{j1}X_1 + A_{j2}X_2, \quad Y_j' = B_{j1}Y_1 + B_{j2}Y_2 \quad (j = 1, 2),$$

where $$A_{jk} = \alpha_{jk} - i\gamma_{jk}, \quad B_{jk} = \alpha_{jk} + i\gamma_{jk} \qquad (j, k = 1, 2).$$

Also $$\xi_1^2 + \eta_1^2 + \xi_2^2 + \eta_2 = X_1 Y_1 + X_2 Y_2.$$

If -1 be a square in the $GF[p^n]$. $p > 2$, the substitution (4) is a dualistic substitution belonging to the field, the substitution on the Y_1, Y_2 being reciprocal to that on the X_1, X_2. Hence there are $(p^{2n}-1)(p^{2n}-p^n)$ substitutions (4); so that M_1M_2 is one of $p^{3n}(p^{2n}+1)(p^n+1)$ conjugate substitutions within $SA\ (4, p^n)$.

---

* The simplifications arise since $M_1 M_2$ takes the form $T_{1,-i} T_{2,-i}$.

If -1 be a not-square in the $GF[p^n]$, then $i^{p^n} = -i$; so that

$$X_j^{p^n} = Y_j, \quad A_{jk}^{p^n} = B_{jk}, \quad X_1Y_1+X_2Y_2 = X_1^{p^n+1}+Y_1^{p^n+1}.$$

Hence (4) is defined by the general substitution

$$X_j' = A_{j1}+A_{j2}X_2 \qquad (j=1,2)$$

of the hyperorthogonal group on two indices having the order $p^n(p^{2n}-1)(p^n+1)$. Hence M_1M_2 is one of $p^{3n}(p^{2n}+1)(p^n-1)$ conjugate substitutions within $SA\ (4, p^n)$.

Within $SA\ (4, p^n)$ *there are exactly three sets of conjugate substitutions of period* 4, *represented by* M_1, $M_1T_{1,-1}T_{2,-1}$, *and* M_1M_2, *respectively. Each set contains* $p^{3n}(p^{2n}+1)(p^n+\epsilon)$ *substitutions, where* $\epsilon = \pm 1$ *according as* $p^n = 4l \pm 1$.

Quaternary Abelian Substitutions of period 8.

5. If $SA\ (4, p^n)$ contains a substitution S whose square is M_1M_2, then S must be commutative with M_1M_2, and hence be of the form (2). The condition $S = S^{-1}M_1M_2$ gives readily

$$\alpha_{11} = \gamma_{11}, \quad \alpha_{12} = \gamma_{21}, \quad \alpha_{21} = \gamma_{12}, \quad \alpha_{22} = \gamma_{22}.$$

Relations (3) then become, for $p > 2$,

$$\alpha_{22}^2 = \alpha_{11}^2, \qquad (\alpha_{11}+\alpha_{22})(\alpha_{12}-\gamma_{12}) = 0,$$

$$2\alpha_{11}^2+\alpha_{12}^2+\gamma_{12}^2 = 1, \qquad (\alpha_{11}+\alpha_{22})(\alpha_{12}+\gamma_{12}) = 0.$$

If $\alpha_{11}+\alpha_{22} \neq 0$, then $\alpha_{11} = \alpha_{22}$, $\alpha_{12} = \gamma_{12} = 0$. Hence must 2 be a square in the $GF[p^n]$, in which case the required substitutions are

$$\left\{\begin{matrix} \alpha & \alpha & 0 & 0 \\ -\alpha & \alpha & 0 & 0 \\ 0 & 0 & \alpha & \alpha \\ 0 & 0 & -\alpha & \alpha \end{matrix}\right\} \qquad (\alpha^2 = \tfrac{1}{2}),$$

the square of which is indeed M_1M_2.

There remains the case $\alpha_{11}+\alpha_{22}=0$, when S becomes

$$(5)\quad \begin{Bmatrix} \alpha & \alpha & \alpha_{12} & \gamma_{12} \\ -\alpha & \alpha & -\gamma_{12} & \alpha_{12} \\ \gamma_{12} & \alpha_{12} & -\alpha & -\alpha \\ -\alpha_{12} & \gamma_{12} & \alpha & -\alpha \end{Bmatrix} \quad (2\alpha^2+\alpha_{12}^2+\gamma_{12}^2=1).$$

Consider the case $p^n=3$. If $S^2=M_1M_2$, S must have the form (5). If $\alpha=0$, then $\alpha_{12}^2+\gamma_{12}^2=1$; so that either $\alpha_{12}=0$ or $\beta_{12}=0$. The two cases are interchanged if we transform by M_2. Setting therefore $\gamma_{12}=0$, $\alpha=0$, $\alpha_{12}^2=1$, and transforming (5) by $T_{2,\alpha_{12}}^{-1}$, we obtain

$$M_1P_{12}\equiv\begin{Bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{Bmatrix}.$$

If $\alpha\neq 0$, then $\alpha_{12}^2+\gamma_{12}^2=-1$; so that $\alpha_{12}^2\equiv\gamma_{12}^2\equiv 1 \pmod 3$. Transforming by $T_{2,-\gamma_{12}}$, we may suppose that $\gamma_{12}=-1$ in (5). Transforming by M_2^3, the case $\alpha_{12}=-1$ is reduced to the case $\alpha_{12}=+1$. The resulting substitution (5), given by $\alpha=-1$, is transformed by $P_{12}T_{2,-1}$ into a similar one with $\alpha=+1$, viz.,

$$\begin{Bmatrix} 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \end{Bmatrix}.$$

This is transformed into M_1P_{12} by the Abelian substitution

$$\begin{Bmatrix} -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \end{Bmatrix}.$$

Combining the present result with that of § 3, it follows that *every substitution of period* 8 of $SA\,(4, 3)$ *is conjugate within the latter with* M_1P_{12}.

6. Theorem.—*Within $SA(4, 3)$, the substitution M_1P_{12} of period 8 is commutative only with its powers.*

The identity $SM_1P_{12} = M_1P_{12}S$ requires that S have the form

$$\left\{\begin{matrix} \alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12} \\ -\gamma_{11} & \alpha_{11} & -\gamma_{12} & \alpha_{12} \\ -\gamma_{12} & \alpha_{12} & \alpha_{11} & \gamma_{11} \\ -\alpha_{12} & -\gamma_{12} & -\gamma_{11} & \alpha_{11} \end{matrix}\right\},$$

subject to the Abelian conditions, which reduce to the two

$$\alpha_{11}^2+\gamma_{11}^2+\alpha_{12}^2+\gamma_{12}^2 = 1, \quad \alpha_{11}(\alpha_{12}-\gamma_{12})+\gamma_{11}(\alpha_{12}+\gamma_{12}) = 0.$$

If $\alpha_{11} = \gamma_{11} = 0$, the four sets of solutions modulo 3 of $\alpha_{12}^2+\gamma_{12}^2 = 1$ give four substitutions. If $\alpha_{11} = 0$, $\gamma_{11} \neq 0$, then $\alpha_{12} = -\gamma_{12} = 0$; if $\alpha_{11} \neq 0$, $\gamma_{11} = 0$, then $\alpha_{12} = \gamma_{12} = 0$. If α_{11} and γ_{11} are $\neq 0$, either $\alpha_{11} = \gamma_{11}$, so that $\alpha_{12} = 0$, or $\alpha_{11} = -\gamma_{11}$, so that $\gamma_{12} = 0$; but in either case the first Abelian condition is not satisfied. The resulting eight substitutions commutative with M_1P_{12} must be its eight powers.

Corollary I. *$SA(4, 3)$ contains no substitution of period 16.*—Indeed, the square of such a substitution would be of period 8, and hence be conjugate with M_1P_{12} by § 5. But, for $S^2 = M_1P_{12}$, S would be commutative with M_1P_{12}, and hence be a power of the latter.

Corollary II. *Within $SA(4, 3)$, every cyclic sub-group of order 8 is self-conjugate in exactly a group of order 32.*—Such a sub-group is conjugate with that generated by $V \equiv M_1P_{12}$. But V is conjugate with $V^3 \equiv T_{1,-1}M_2P_{12}$, $V^5 = M_1P_{12}T_{1,-1}T_{2,-1}$, and $V^7 = T_{2,-1}M_2P_{12}$, each of period 8 (§ 5). To verify this result, we may transform V into V^3, V^5, V^7 by, respectively, A, $T_{2,1}$, $AT_{2,-1}$, where A denotes the following substitution of period 2 belonging to $SA(4, 3)$:—

$$\left\{\begin{matrix} 0 & 0 & -1 & -1 \\ 0 & 0 & -1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \end{matrix}\right\}.$$

7. Theorem.—*There are exactly four sets of conjugate substitutions of period 3 in the group $SA(4, 3^n)$.*

Within $SA\,(4, p^n)$ every substitution is conjugate with one of the following types:—*

$$\Sigma = \begin{Bmatrix} \alpha & \gamma & 0 & 0 \\ \beta & \delta & 0 & 0 \\ 0 & 0 & \alpha_{22} & \gamma_{22} \\ 0 & 0 & \beta_{22} & \delta_{22} \end{Bmatrix}, \quad A = \begin{Bmatrix} \alpha & \gamma & 1 & 0 \\ \beta & \delta & 0 & \rho \\ \alpha_{21} & \gamma_{21} & \alpha_{22} & \gamma_{22} \\ \beta_{21} & \delta_{21} & \beta_{22} & \delta_{22} \end{Bmatrix}.$$

If A be of period 3, $A^2 = A^{-1}$, giving

$$\begin{Bmatrix} \alpha^2+\beta\gamma+\alpha_{21} & \alpha\gamma+\delta\gamma+\gamma_{21} & \alpha+\alpha_{22} & \rho\gamma+\gamma_{22} \\ \beta\alpha+\beta\delta+\rho\beta_{21} & \beta\gamma+\delta^2+\rho\delta_{21} & \beta+\rho\beta_{22} & \rho\delta+\rho\delta_{22} \\ \dots & \dots & \dots & \dots \end{Bmatrix} = \begin{Bmatrix} \delta & -\gamma & \delta_{21} & -\gamma_{21} \\ -\beta & \alpha & -\beta_{21} & \alpha_{21} \\ \dots & \dots & \dots & \dots \end{Bmatrix}.$$

The following are therefore necessary conditions:—

$$(6) \quad \begin{cases} \alpha_{21} = \delta-\alpha^2-\beta\gamma, & \rho\beta_{21} = -\beta-\beta\alpha-\beta\delta, \\ \gamma_{21} = -\gamma-\alpha\gamma-\delta\gamma, & \rho\delta_{21} = \alpha-\delta^2-\beta\gamma, \\ \alpha_{22} = \delta_{21}-\alpha, & \rho\beta_{22} = -\beta_{21}-\beta, \\ \gamma_{22} = -\gamma_{21}-\rho\gamma, & \rho\delta_{22} = \alpha_{21}-\rho\delta. \end{cases}$$

The Abelian relations require

$$(7) \quad \alpha\delta-\beta\gamma+\rho = 1,$$

and

$$\alpha_{21}\delta_{21}-\beta_{21}\gamma_{21}+\alpha\delta-\beta\gamma = 1.$$

Let, first, $\rho \neq 0$. The second relation becomes, by (6) and (7),

$$(8) \quad (\alpha+\delta)^3+3(\alpha+\delta+1)(\rho-1)+1 = 0.$$

For $p = 3$, this gives $(\alpha+\delta+1)^3 = 0$. We limit the discussion to the case

$$(9) \quad \alpha+\delta+1 = 0.$$

Applying (6) and (9), A takes the form

$$A' \equiv \begin{Bmatrix} \alpha & \gamma & 1 & 0 \\ \beta & \delta & 0 & \rho \\ -\rho & 0 & \delta & -\rho\gamma \\ 0 & -1 & -\beta\rho^{-1} & \alpha \end{Bmatrix} \quad (\alpha\delta-\beta\gamma+\rho = 1).$$

For any $GF\,[p^n]$, A' is an Abelian substitution of period 3.

If $\beta \neq 0$, A' is transformed into a substitution of the form Σ by the special Abelian substitution

$$N_{1,\,2,\,\rho\beta^{-1}}: \quad \xi_1' = \xi_1+\rho\beta^{-1}\eta_2, \quad \xi_2' = \xi_2+\rho\beta^{-1}\eta_1.$$

---

* Dickson, *Quarterly Journal*, Vol. XXXII., § 5, p. 51.

If $\gamma \neq 0$, the transformed of A' by $M_1^3 M_2 P_{12}$ is of the form A' with $\beta \neq 0$.

Finally, if $\beta = \gamma = 0$, the transformed of A' by $Q_{1,2,\alpha\rho^{-1}} T_{2,\rho^{-1}}$ gives

$$\left\{\begin{array}{rrrr} 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ -1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \end{array}\right\}.$$

This is transformed into Σ_1 by S_1 belonging to $SA\,(4, p^n)$, where

$$\Sigma_1 = \left\{\begin{array}{rrrr} 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & -1 \end{array}\right\}, \quad S_1 = \left\{\begin{array}{rrrr} 1 & -1 & 0 & 1 \\ 0 & 0 & -1 & 1 \\ 1 & 0 & 1 & -1 \\ -1 & 1 & 0 & 0 \end{array}\right\}.$$

Hence, if A be an Abelian substitution in the $GF\,[p^n]$ satisfying (9) and having $\rho \neq 0$, it is conjugate within $SA\,(4, p^n)$ with a substitution Σ.

For $\rho = 0$, relations (6) give

$$\alpha_{21} = \delta - \alpha^2 - \beta\gamma = 0, \quad \alpha - \delta^2 - \beta\gamma = 0, \quad \beta\,(1 + \alpha + \delta) = 0.$$

Subtracting the second from the first, $(\delta - \alpha)(\alpha + \delta + 1) = 0$. Hence, if $\alpha + \delta + 1 \neq 0$, $\delta = \alpha$, $\beta = 0$, $\alpha = \delta^2$. Then (7) requires $\alpha = \delta = 1$; so that $\alpha + \delta + 1 \equiv 0 \pmod 3$. Hence (9) must hold if $p = 3$; when A becomes

$$\left\{\begin{array}{cccc} \alpha & \gamma & 1 & 0 \\ \beta & \delta & 0 & 0 \\ 0 & 0 & \delta_{21} - \alpha & 0 \\ -\beta & \delta_{21} & \beta_{22} & \delta_{22} \end{array}\right\} \quad [\delta_{22}(\delta_{21} - \alpha) = 1].$$

If it has period 3, $(\delta_{21} - \alpha)^2 = \delta_{21} - \alpha$; so that $\delta_{21} - \alpha = 1$, $\delta_{22} = 1$. The resulting substitution is of period 3 if, and only if, $\beta = 3\beta_{22}$. For $p = 3$, $\beta = 0$, $\alpha\delta = 1$, $\alpha + \delta = -1$. Hence $\alpha^2 + \alpha + 1 = 0$, $\alpha^3 = 1$; so that $\alpha = 1$ in the $GF\,[3^n]$. The resulting substitution is

$$A_1 = \left\{\begin{array}{cccc} 1 & \gamma & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & \beta_2 & 1 \end{array}\right\}.$$

If $\beta_2 \neq 0$, A_1 is transformed into a substitution Σ by

$$\xi_1' = \xi_1 + \tau\eta_2, \quad \xi_2' = \xi_2 + \tau\eta_1, \qquad 1 + \tau\beta_2 = 0.$$

If $\gamma \neq 0$, the transformed of A_1 by $M_1^3 M_2 P_{12}$ is of the form A_1 with $\beta_2 \neq 0$. Finally, if $\gamma = \beta_2 = 0$, $A_1 \equiv Q_{1,2,1}$ is transformed into $L_{1,1} L_{2,-1}$ of the form Σ by the Abelian substitution

$$\left\{\begin{matrix} -1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \\ -1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{matrix}\right\}.$$

Within $SA\,(4, 3^n)$ every substitution of period 3 is therefore conjugate with a substitution of the form Σ.

The substitution Σ is the product of two substitutions

$$\Sigma' \equiv \left\{\begin{matrix} \alpha & \gamma \\ \beta & \delta \end{matrix}\right\}, \quad \Sigma'' \equiv \left\{\begin{matrix} \alpha_{22} & \gamma_{22} \\ \beta_{22} & \delta_{22} \end{matrix}\right\},$$

the former affecting only the indices ξ_1, η_1, and the latter affecting only ξ_2, η_2. Since Σ' and Σ'' are commutative, each must be of period 3 if Σ shall have period 3; also each must be of determinant unity if their product Σ is to be Abelian. But, in any field, Σ' is of period 3 if, and only if, $\alpha + \delta = -1$. Supposing $\alpha + \delta = -1$, we have the following two cases:—

If $\beta \neq 0$, Σ' is transformed into $L_{1,-\beta}$ by the substitution

$$\left\{\begin{matrix} 0 & -1 \\ 1 & (\alpha - \delta)/\beta \end{matrix}\right\}.$$

If $\beta = 0$, then $\alpha\delta = 1$ and $\alpha + \delta = -1$ require that $\alpha = \delta = 1$ in the $GF[3^n]$; so that $\Sigma' = L_{1,\gamma}$. In either case, Σ' is conjugate with a substitution $L_{1,\tau}$. The latter is transformed into $L_{1,\tau\kappa^2}$ by $T_{1,\kappa}$; so that Σ' is conjugate either with $L_{1,1}$ or with $L_{1,\nu}$, where ν is a particular not-square.

Applying a similar reduction to Σ'', it follows that, within $SA\,(4, 3^n)$, every substitution of period 3 is conjugate with one of the substitutions $L_{1,1}$, $L_{1,\nu}$, $L_{1,1} L_{2,1}$, $L_{1,\nu} L_{2,1}$, $L_{1,\nu} L_{2,\nu}$. But $L_{1,1} L_{2,1}$ is transformed into $L_{1,\nu} L_{2,\nu}$ by the substitution

$$\left\{\begin{matrix} \nu\delta & 0 & \nu\sigma & 0 \\ 0 & \delta & 0 & \sigma \\ -\nu\sigma & 0 & \nu\delta & 0 \\ 0 & -\sigma & 0 & \delta \end{matrix}\right\},$$

which belongs to $SA\,(4, p^n)$ if $\nu(\delta^2 + \sigma^2) = 1$, a relation having solutions in every $GF[p^n]$. Of the remaining types $L_{1,1}$, $L_{1,\nu}$, $L_{1,1} L_{2,1}$, and $L_{1,\nu} L_{2,1}$, it is readily proven that no two are conjugate within $SA\,(4, p^n)$.

8. The method employed in §§ 2–6 may be extended to determine representative substitutions S within $SA\,(4, p^n)$, $p > 2$, of each set of conjugate substitutions whose period is an even integer $2a$, the case a odd being excluded if $S^a = T$, the self-conjugate substitution. In the excluded case, $(ST)^a = I$, a being odd. Hence the method applies to all substitutions S for which S and ST are of even period. Since S^a is of period 2 by hypothesis, it is conjugate within $SA\,(4, p^n)$ either with $T_{1,-1}$ or else with T, in the latter case $S^{\frac{1}{2}a}$ being conjugate with $M_1 M_2$ (§ 2). Hence, by a suitable transformation within $SA\,(4, p^n)$, $p > 2$, we may give to S a form having among its powers either $T_{1,-1}$ or else $M_1 M_2$.

In the first case, S is commutative with $T_{1,-1}$; so that S has the form Σ of § 7. Then $S = \Sigma' \Sigma''$, where Σ' and Σ'' are binary substitutions of determinant unity. Each is known to be of period a divisor of $2p$ or of $p^n \pm 1$. Hence S is of period 2, $2p$, $2d_{\mp}$, $2pd_{\mp}$, or $d_{\mp} d'_{\mp}$, where $d_{\mp}$ and $d'_{\mp}$ are divisors of $p^n \mp 1$.

In the second case, S is commutative with $M_1 M_2$; so that S has the form (2). As in § 4, the problem reduces to the study of binary linear substitutions in the $GF\,[p^n]$ or of binary hyperorthogonal substitutions in the $GF\,[p^{2n}]$, according as respectively -1 is a square or a not-square in the $GF\,[p^n]$.

9. For $p^n = 3$, the substitutions Σ' of determinant unity form a group G_{24} composed of the identity $T_{1,-1}$, 8 substitutions conjugate with $L_{1,\pm 1}$ within G_{24}, 6 conjugate with M_1, and 8 conjugate with $L_{1,\pm 1} T_{1,-1}$. Hence, within $SA\,(4, 3)$ a substitution of period 6, a power of which is conjugate with $T_{1,-1}$, is itself conjugate with one of the substitutions

$$L_{1,\pm 1} T_{1,-1}, \quad L_{2,\pm 1} T_{1,-1}, \quad L_{1,\pm 1} L_{2,1} T_{1,-1}, \quad L_{1,\pm 1} L_{2,-1} T_{1,-1}.$$

Within $SA\,(4, 3)$ a substitution of period 12, a power of which is conjugate with $T_{1,-1}$, is itself conjugate with $M_2 L_{1,\pm 1}$ or $M_2 L_{1,\pm 1} T_{1,-1}$, the latter being conjugate with

$$M_2^3 L_{1,\pm 1} T_{1,-1} \equiv M_2 L_{1,\pm 1} T_{1,-1} T_{2,-1}.$$

Together with the substitutions of periods 2 and 4, determined in § 2, the present enumeration is seen to give all types of substitutions of $SA\,(4, 3)$ having among their powers substitutions conjugate with $T_{1,-1}$.

Considering next those substitutions having one of their powers conjugate with $M_1 M_2$, we find the representatives $M_1 M_2$, $M_1 P_{12}$, and $P_{12} L_{1,-1} T_{1,-1}$, whose first, second, and third powers respectively are conjugate with $M_1 M_2$.

It remains to determine representatives of the substitutions of odd period. The case of period 3 has been completely determined in § 7. The substitutions of SA (4, 3)

$$H_5 \equiv \begin{Bmatrix} 1 & 1 & 1 & 0 \\ -1 & 0 & 0 & 0 \\ -1 & 0 & 1 & -1 \\ 0 & 0 & 1 & 0 \end{Bmatrix}, \qquad N_9 \equiv \begin{Bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 1 & -1 \end{Bmatrix}$$

are of periods 5 and 9 respectively. Every substitution of period 5 is conjugate with H_5; every one of period 9 is conjugate with N_9 or N_9^{-1}. The only odd periods possible are 3, 5, 9. These statements are not proven here; a verification of them results from the fact that the following table exhibits 51840 distinct substitutions of SA (4, 3) of order 51840.

Types.	Period.	Number of Conjugates to each type.
Identity	1	1
$T \equiv T_{1,-1} T_{2,-1}$	2	1
$T_{1,-1}$	2	90
$L_{1,\pm 1}$	3	40
$L_{1,\pm 1} T$	6	40
$L_{1,1} L_{2,1}$	3	240
$L_{1,-1} L_{2,1}$	3	480
$L_{1,1} L_{2,1} T$	6	240
$L_{1,-1} L_{2,1} T$	6	480
$M_1, \quad M_1 T$	4	540
$M_1 M_2$	4	540
$M_2 L_{1,\pm 1}, \quad M_2 L_{1,\pm 1} T$	12	2160
$L_{1,\pm 1} T_{1,-1}, \quad L_{1,\pm 1} T_{2,-1}$	6	360
$L_{1,1} L_{2,\pm 1} T_{1,-1}$	6	1440
$L_{1,-1} L_{2,\pm 1} T_{1,-1}$	6	1440
$M_1 P_{12}$	8	6480
$P_{12} L_{1,-1} T_{1,-1}$	12	4320
H_5	5	5184
$H_5 T$	10	5184
$N_9, \quad N_9^{-1}$	9	2880
$N_9 T, \quad N_9^{-1} T$	18	2880

*A Group of definition analogous to that of the Abelian Linear Group.**

10. Consider the group G of linear substitution S which, when operating cogrediently upon two sets of variables ξ_i, η_i and $\bar{\xi}_i$, $\bar{\eta}_i$, effect a linear transformation of the functions

$$\Delta_1 \equiv \begin{vmatrix} \xi_1 & \eta_1 \\ \bar{\xi}_1 & \bar{\eta}_1 \end{vmatrix}, \qquad \Delta_2 \equiv \begin{vmatrix} \xi_2 & \eta_2 \\ \bar{\xi}_2 & \eta_2 \end{vmatrix}.$$

Now S replaces Δ_1 by

$$\begin{vmatrix} \alpha_{11} & \gamma_{11} \\ \beta_{11} & \delta_{11} \end{vmatrix} \Delta_1 + \begin{vmatrix} \alpha_{11} & \alpha_{12} \\ \beta_{11} & \beta_{12} \end{vmatrix} \begin{vmatrix} \xi_1 & \xi_2 \\ \bar{\xi}_1 & \bar{\xi}_2 \end{vmatrix} + \begin{vmatrix} \alpha_{11} & \gamma_{12} \\ \beta_{11} & \delta_{12} \end{vmatrix} \begin{vmatrix} \xi_1 & \eta_2 \\ \bar{\xi}_1 & \bar{\eta}_2 \end{vmatrix}$$

$$+ \begin{vmatrix} \alpha_{12} & \gamma_{12} \\ \beta_{12} & \delta_{12} \end{vmatrix} \Delta_2 + \begin{vmatrix} \gamma_{11} & \alpha_{12} \\ \delta_{11} & \beta_{12} \end{vmatrix} \begin{vmatrix} \eta_1 & \xi_2 \\ \bar{\eta}_1 & \bar{\xi}_2 \end{vmatrix} + \begin{vmatrix} \gamma_{11} & \gamma_{12} \\ \delta_{11} & \delta_{12} \end{vmatrix} \begin{vmatrix} \eta_1 & \eta_2 \\ \bar{\eta}_1 & \bar{\eta}_2 \end{vmatrix}.$$

Hence, if S replace Δ_1 by $\lambda_{11}\Delta_1 + \lambda_{12}\Delta_2$ and Δ_2 by $\lambda_{21}\Delta_1 + \lambda_{22}\Delta_2$,

$$(10) \quad \begin{cases} \begin{vmatrix} \alpha_{ij} & \gamma_{ij} \\ \beta_{ij} & \delta_{ij} \end{vmatrix} = \lambda_{ij}, \quad \begin{vmatrix} \alpha_{i1} & \alpha_{i2} \\ \beta_{i1} & \beta_{i2} \end{vmatrix} = 0, \quad \begin{vmatrix} \alpha_{i1} & \gamma_{i2} \\ \beta_{i1} & \delta_{i2} \end{vmatrix} = 0, \\ \qquad\qquad\qquad \begin{vmatrix} \gamma_{i1} & \gamma_{i2} \\ \delta_{i1} & \delta_{i2} \end{vmatrix} = 0, \quad \begin{vmatrix} \alpha_{i2} & \gamma_{i1} \\ \beta_{i2} & \delta_{i1} \end{vmatrix} = 0, \end{cases}$$

holding for $i, j = 1, 2$. In view of these relations, the inverse of S is the product of a substitution multiplying every index by the reciprocal of the determinant of S by the substitution

$$\left\{ \begin{matrix} \lambda_{22}\delta_{11}, & -\lambda_{22}\gamma_{11}, & \lambda_{12}\delta_{21}, & -\lambda_{12}\gamma_{21} \\ -\lambda_{22}\beta_{11}, & \lambda_{22}\alpha_{11}, & -\lambda_{12}\beta_{21}, & \lambda_{12}\alpha_{21} \\ \lambda_{21}\delta_{12}, & -\lambda_{21}\gamma_{12}, & \lambda_{11}\delta_{22}, & -\lambda_{11}\gamma_{22} \\ -\lambda_{21}\beta_{12}, & \lambda_{21}\alpha_{12}, & -\lambda_{11}\beta_{22}, & \lambda_{11}\alpha_{22} \end{matrix} \right\}.$$

The derivation of S^{-1} from S is quite similar to the derivation of the reciprocal of an Abelian linear substitution.

We proceed to prove that either $\lambda_{12} = \lambda_{21} = 0$ or else $\lambda_{11} = \lambda_{22} = 0$.

---

* An Abelian substitution replaces $\Delta_1 + \Delta_2$ by $\mu\Delta_1 + \mu\Delta_2$. Consider a group of substitutions S_1, S_2, ..., which replace $\Delta_1 + \Delta_2$ by $\tau\Delta_1 + \mu\Delta_2$, τ and μ depending on the particular substitution. Suppose that, for S_1, $\mu = \tau + \kappa$, $\kappa \neq 0$. Since $S_1 S_2$ belongs to the group, S_2 must replace $\kappa\Delta_2$ by a linear function of Δ_1 and Δ_2. Hence the group is that denoted by G in the text.

Among the relations (10) occur the following :—

$$\left\{\begin{aligned} &\alpha_{i1}\beta_{i2}-\beta_{i1}\alpha_{i2}=0,\\ &\gamma_{i1}\beta_{i2}-\delta_{i1}\alpha_{i2}=0,\end{aligned}\right. \qquad \left\{\begin{aligned} &\alpha_{i1}\delta_{i2}-\beta_{i1}\gamma_{i2}=0,\\ &\gamma_{i1}\delta_{i2}-\delta_{i1}\gamma_{i2}=0.\end{aligned}\right.$$

If the determinant $\lambda_{i1}\equiv\alpha_{i1}\delta_{i1}-\beta_{i1}\gamma_{i1}\neq 0$, then will $\beta_{i2}=\alpha_{i2}=\delta_{i2}=\gamma_{i2}=0$, and therefore $\lambda_{i2}=0$. Hence, either S has the form

$$\Sigma\equiv\left\{\begin{matrix} \alpha_{11} & \gamma_{11} & 0 & 0\\ \beta_{11} & \delta_{11} & 0 & 0\\ 0 & 0 & \alpha_{22} & \gamma_{22}\\ 0 & 0 & \beta_{22} & \delta_{22}\end{matrix}\right\}.$$

and replaces Δ_i by $\lambda_{ii}\Delta_i$, or S has the form $(\xi_1\xi_2)(\eta_1\eta_2)\Sigma$ and replaces Δ_1 by $\lambda_{12}\Delta_2$ and Δ_2 by $\lambda_{21}\Delta_1$. The structure of the group G thus follows from that of the binary group.

Note on Stability of Motion, with an application to Hydrodynamics.

By T. J. I'A. BROMWICH. Communicated February 14th, 1901. Received, in revised form, April 5th, 1901.

The following note on stability was, in the first place, suggested by a result of Prof. Klein's, given in his lectures at Princeton (1896), relating to the stability of a top spinning in a nearly vertical position, thus:—

The theory of small oscillations gives a certain limiting (or critical) value (n_0) for the spin (n) of the top; and, if $n<n_0$, it would seem that the top is necessarily unstable; further, if $n=n_0$, Routh states that the top is unstable. Hence, if we suppose n to diminish continuously past the value n_0, there would be an abrupt change from stability to instability. But Klein showed that, for *small* values of $(n-n_0)$, the amplitude of the deviation of the axis from the vertical produced by a given small disturbance does not depend on the sign of $(n-n_0)$; and, in this sense, *practical* stability exists for values of n slightly less than n_0, though theoretical stability is lost. Further, Klein proved that the critical case $n=n_0$ is really stable.

In what follows I attempted in the first place to discuss a slightly generalized form of equation, which includes as special cases Klein's results for the top and the hydrodynamical problem of a solid possessing helicoidal symmetry moving through an infinite frictionless liquid. This and the details of the hydrodynamical problem made up the note as presented to the Society last February.

At the March meeting, Prof. Love (who was one of the referees of my note) read an informal paper on the question of stability of motion generally, which he has kindly put at my disposal; from this I have made some extracts (notably, his definitions of stability); and his remarks have led me to amplify the discussion of general stability, so that this part of my note is considerably longer than it was originally. The other referee pointed out that, as the complete solution both of the top and of the hydrodynamical problem is known in terms of elliptic functions, it might be more convincing to use the known results in establishing my conclusions: this advice I have not followed, as it seemed best to make the note, as far as possible, depend only on dynamical principles. Besides, it is conceivable that cases may arise to which my results could apply without being capable of exact integration by means of elliptic functions or otherwise. I must thank both referees for taking considerable trouble and devoting much time to the careful examination of my work.

The following *definitions of stability* are extracted from an unpublished manuscript by Prof. Love:—

"We seek a precise definition of *instability*, as easier to express than a definition of stability. We compare the disturbed and undisturbed motions. Let θ be any coordinate of the system, $\Delta\theta$ the difference between the values of θ at time t in the disturbed and undisturbed motions; call the set of quantities of type $\Delta\theta$ *the displacement*. Let $\Delta\Theta$ be the difference between the initial impulses (corresponding to θ) in the disturbed and undisturbed motions; call the set of quantities of type $\Delta\Theta$ *the disturbance*. Let a be a suitably chosen finite quantity (which may be as small as we please). Then—

"*If, however small the disturbance (i.e., all the $\Delta\Theta$'s) may be, a value of t can be found for which the displacement (i.e., any $\Delta\theta$) exceeds a, the motion is unstable.*

"When the motion is not, in this sense, unstable, there is *complete stability.*

"Again let P be any point of the disturbed path of any particle of the system, P' *the nearest point* of the undisturbed path, r the distance

PP', v the excess of the velocity at P in the disturbed path above that at P' in the undisturbed path; α, β suitably chosen finite quantities (as small as we please). Then—

"*If, however small the disturbance may be, a value of t can be found for which any r exceeds α or any v exceeds β, there is instability of path.*"

An Attempt to Discuss the Stability of a State of Steady Motion.

We shall use the Hamiltonian equations and can choose all the coordinates (x) and momenta (ξ) so as to vanish in the steady motion; then (unless the steady motion is critical in the analytical sense) the Hamiltonian function can be put in the form

$$H = H^0 + H^1 + H^2 + H^3 + \ldots,$$

where each term is homogeneous in the coordinates and the momenta and is of the degree indicated by the index attached to it; this series will converge absolutely and uniformly provided that $|x|$ and $|\xi|$ do not exceed certain limits. In order that the steady motion may be dynamically possible H^1 must vanish, for the canonical equations must be satisfied by zero values of the coordinates and momenta.

The method of "small oscillations" is contented with the first approximation to the equations of motion given by

$$\frac{dx_r}{dt} = \frac{\partial H^2}{\partial \xi_r}, \quad \frac{d\xi_r}{dt} = -\frac{\partial H^2}{\partial x_r} \quad (r = 1, 2, \ldots, n).$$

If we assume all the coordinates and momenta proportional to $e^{\lambda t}$, we find that as a consequence of these equations λ is a root of an equation

$$\Delta = 0,$$

where Δ is a $2n$-rowed determinant, λ appearing linearly in $2n$ of the elements of Δ, and nowhere else. Thus we have $2n$ values of λ which, in virtue of the properties of Δ, can be grouped in n pairs $\pm\lambda_1, \pm\lambda_2, \ldots, \pm\lambda_n$.

Since the Hamiltonian equations are only a transformed form of the Lagrangian ones, from which Routh starts, it follows that $\pm\lambda_1, \ldots, \pm\lambda_n$ are the roots of Routh's n-rowed determinantal equation (in which every element is quadratic in λ).

Now, in a paper accepted by the Society at the March meeting (p. 198 of this volume), I have shown that a linear transformation of the coordinates and momenta can be found such that

$$H^2 = \Sigma \lambda_r x_r \xi_r \quad (r = 1, 2, \ldots, n)$$

and of such a character that the canonical equations of motion are not altered in form by the substitution. If the roots of $\Delta = 0$ are not all different, the invariant-factors of Δ must be linear,* in order that this form for H^2 may be correct. Making the same substitution on the whole of H, we shall have now

$$H = H^0 + \Sigma \lambda_r x_r \xi_r + H^3 + H^4 + \dots,$$

with the equations of motion

$$\frac{dx_r}{dt} = \frac{\partial H}{\partial \xi_r}, \quad \frac{d\xi_r}{dt} = -\frac{\partial H}{\partial x_r}.$$

We make the hypothesis that $\lambda_1, \dots, \lambda_n$ are pure imaginaries, and we shall prove that, under certain other restrictions, the equations can be solved in converging series. We follow the investigation used by Poincaré (*Mécanique Céleste*, t. I, chap. vii.) for the case of asymptotic solutions.

The equations of motion take the form

$$\frac{dx_r}{dt} = \lambda_r x_r + \frac{\partial H^3}{\partial \xi_r} + \frac{\partial H^4}{\partial \xi_r} + \dots = \lambda_r x_r + K_r^2 + K_r^3 + \dots,$$

$$\frac{d\xi_r}{dt} = -\lambda_r x_r - \frac{\partial H^3}{\partial x_r} - \frac{\partial H^4}{\partial x_r} - \dots = -\lambda_r \xi_r + L_r^2 + L_r^3 + \dots,$$

where, as before, the indices indicate the degree of the terms to which they are attached.

The first approximation is found by leaving out all the K's and L's, so that we find

$$x_r = a_r e^{\lambda_r t}, \quad \xi_r = \alpha_r e^{-\lambda_r t},$$

where the a's and α's are constants of integration, whose values are determined by the initial disturbance, and so $|a|$, $|\alpha|$ may be taken as small as may be convenient; for, in discussions of stability, the initial disturbance is to be at our disposal in magnitude, though arbitrary in species. We now endeavour to find series for x_r, ξ_r expressed in powers of $a_r e^{\lambda_r t}$, $\alpha_r e^{-\lambda_r t}$; so assume

$$x_r = x_r^1 + x_r^2 + x_r^3 + \dots,$$

$$\xi_r = \xi_r^1 + \xi_r^2 + \xi_r^3 + \dots,$$

---

* That is, if a factor $(\lambda - e)$ appears *exactly* p times in Δ, it must appear *exactly* $(p-1)$ times in the H.C.F. of all the first minors of Δ; so that in at least one first minor $(\lambda - e)$ appears *exactly* $(p-1)$ times, while it *may* appear more than $(p-1)$ times in the others.

where x_r^p, ξ_r^p represent all the terms of x_r, ξ_r respectively which are of degree p in the a's and α's. Then, on substituting, each K and L can be sub-divided, thus

$$K_r^p = K_r^{p,p} + K_r^{p,p+1} + K_r^{p,p+2} + \dots,$$

where $K_r^{p,q}$ denotes that part of K_r^p which is of degree q $(\geqq p)$ in the a's and α's.

Substituting in the equations of motion, we have

$$\frac{dx_r^1}{dt} = \lambda_r x_r^1 \quad \text{or} \quad x_r^1 = a_r e^{\lambda_r t},$$

$$\frac{dx_r^2}{dt} - \lambda_r x_r^2 = K_r^{2,2},$$

$$\frac{dx_r^3}{dt} - \lambda_r x_r^3 = K_r^{2,3} + K_r^{3,3},$$

$$\dots \quad \dots \quad \dots \quad \dots$$

$$\frac{dx_r^q}{dt} - \lambda_r x_r^q = K_r^{2,q} + K_r^{3,q} + \dots + K_r^{q,q} = M_r^q, \text{ say,}$$

and

$$\frac{d\xi_r^1}{dt} = -\lambda_r \xi_r^1 \quad \text{or} \quad \xi_r^1 = \alpha_r e^{-\lambda_r t},$$

$$\frac{d\xi_r^2}{dt} + \lambda_r \xi_r^2 = L_r^{2,2},$$

$$\dots \quad \dots \quad \dots$$

$$\frac{d\xi_r^q}{dt} + \lambda_r \xi_r^q = L_r^{2,q} + L_r^{3,q} + \dots + L_r^{q,q} = N_r^q, \text{ say.}$$

From these we calculate successively $x_r^1, \xi_r^1, x_r^2, \xi_r^2, \dots, x_r^q, \xi_r^q, \dots$; for the quantities M_r^q, N_r^q depend only on those x's and ξ's which have indices $1, 2, \dots, q-1$; if we suppose these to have been previously calculated, the value of M_r^q will be of the form

$$M_r^q = \Sigma C a_1^{\theta_1} a_2^{\theta_2} \dots a_n^{\theta_n} \alpha_1^{\phi_1} \alpha_2^{\phi_2} \dots \alpha_n^{\phi_n} \exp\left[t \Sigma \lambda_p (\theta_p - \phi_p)\right],$$

where $\theta_1, \theta_2, \dots, \theta_n, \phi_1, \phi_2, \dots, \phi_n$ are positive integers whose sum is q. Thus, on integrating, we have

$$x_r^q = \Sigma \frac{C a_1^{\theta_1} \dots a_n^{\theta_n} \alpha_1^{\phi_1} \dots \alpha_n^{\phi_n}}{\Sigma \lambda_p (\theta_p - \phi_p) - \lambda_r} \exp\left[t \Sigma \lambda_p (\theta_p - \phi_p)\right],$$

and the expression for ξ_r^q will be similar to this, except that $(+\lambda_r)$

takes the place of $(-\lambda_r)$ in the denominator. Of course, if

$$\lambda_r = \pm \Sigma \lambda_p (\theta_p - \phi_p),$$

one or other of these expressions fails, and powers of t would appear in x_r^q; this indicates that the method of solution adopted gives a result which is only valid for a short time, but it does not *necessarily* imply instability.

It seems impossible to give conditions *necessary* for the convergence of the series

$$x_r^1 + x_r^2 + x_r^3 + \dots ;$$

but it will be possible to find a standard of comparison which will provide *sufficient* conditions. To do this write for brevity

$$b_r = | a_r |, \quad \beta_r = | \alpha_r |,$$

and consider the set of equations

$$\epsilon (y_r - b_r) = \frac{\partial \overline{H}^3}{\partial \eta_r} + \frac{\partial \overline{H}^4}{\partial \eta_r} + \dots,$$

$$\epsilon (\eta_r - \beta_r) = \frac{\partial \overline{H}^3}{\partial y_r} + \frac{\partial \overline{H}^4}{\partial y_r} + \dots,$$

where each $\overline{H}$ is derived from the corresponding H by taking the modulus of every coefficient and replacing the x's by y's and the ξ's by η's. We get, solving the equations, results of the form

$$y_r = \Sigma P \epsilon^{-\delta} b_1^{\theta_1} \dots b_n^{\theta_n} \beta_1^{\phi_1} \dots \beta_n^{\phi_n},$$

where δ is a positive integer, and, as before, $\theta_1, \dots, \theta_n, \phi_1, \dots, \phi_n$ are positive integers whose sum is q. The corresponding term in x_r will be

$$(Q/\pi)\, a_1^{\theta_1} \dots a_n^{\theta_n} \alpha_1^{\phi_1} \dots \alpha_n^{\phi_n} \exp \left[t \Sigma \lambda_p (\theta_p - \phi_p) \right],$$

where $| Q | \overline{\overline{<}} P$ and π is a product of expressions of the type $\left[\Sigma \lambda_p (\theta_p - \phi_p) - \lambda_s\right]$, the number of such expressions being at most equal to δ. It follows that, if the series found for y_r converges, and if none of the divisors $\left[\Sigma \lambda_p (\theta_p - \phi_p) - \lambda_s\right]$ can be less than ϵ, then the modulus of every term in x_r is less than the corresponding term in y_r (for the modulus of the exponential is unity), and so x_r converges absolutely. Exactly the same argument can be applied to ξ_r. If we have an absolutely converging series for x_r, it follows that by sufficiently diminishing $| a_s |$ and $| \alpha_s |$ we can make $| x_r |$ as small as we please; and so the motion is certainly stable for *path*. It is probably not *completely* stable, for reasons which I have indicated in the paper already quoted.

If the invariant-factors of Δ are not linear, we should find powers of t appearing in x_r^1; but it must not be concluded that these necessarily imply instability. All that can be certainly said is that the method of approximation adopted can only be applied for a short time; it may be possible to find another method to give correct values for all time. A good example is that of the top spinning in a vertical position with the "critical" angular velocity; here Δ has squared invariant-factors, and Routh deduced that the position was unstable; but it is really stable, as Klein showed by attacking the problem in another way (see the next paragraph).

The possible introduction of instability through commensurable relations amongst the frequencies was remarked by Routh (*Stability of Motion*, 1877, chap. vii., p. 90).

[*June 27th*, 1901.—In a recent paper, *Annali di Mat.* (Ser. 3), t. v., 1901, p. 221, Levi-Civita has considered the question of instability in a very general way. I have not yet had leisure to compare his results with the foregoing.]

Routh's Minimum-criterion of Stability.

Proceed to the consideration of systems in which certain momenta remain constant. We can eliminate the corresponding velocities from the energy integral, and then obtain a result of the form*

$$T' + K + V = \text{const.},$$

where T' is a positive quadratic form of the other velocities and K is a positive quadratic form of the constant momenta. Thus it follows that, if $(K+V)$ is a *minimum* in the steady motion, that motion is stable (at any rate for path); this condition appears to be *sufficient*, but is not *necessary* in all cases (Routh, *Stability of Motion*, 1877, pp. 83, 84; *cf.* Basset, *Proc. Camb. Phil. Soc.*, Vol. VII., 1892, p. 351); however, if T' contains only *one* velocity, the condition is *necessary and sufficient* (Routh, *loc. cit.*, p. 85).

A good illustration is afforded by the case of the top, in which we have (with Routh's notation)

$$\omega_3 = \text{const.} = n,$$

$$A \sin^2\theta\dot{\psi} + Cn\cos\theta = \text{const.} = Cn,$$

$$A\,(\sin^2\theta\dot{\psi}^2 + \dot{\theta}^2) + 2Mgh\cos\theta = \text{const.} = 2Mgh + Av^2,$$

---

* The important point is that no terms can appear which are bilinear in the velocities and momenta; this fact is fundamental in nearly all theories of reducing quadratic forms, and is the algebraic equivalent of Thomson's and Bertrand's theorems relating to systems started from rest by impulses.

the constants being determined so that $\theta = 0$, $\dot\theta = v$ may satisfy the equations.

Hence $$A\dot\theta^2 + \frac{(Cn)^2}{A}\,\frac{1-\cos\theta}{1+\cos\theta} - 2Mgh\,(1-\cos\theta) = Av^2,$$

or $$K+V = \frac{(Cn)^2}{2A}\,\frac{1-\cos\theta}{1+\cos\theta} - Mgh\,(1-\cos\theta)$$

$$= \frac{(Cn)^2}{8A}\,(\theta^2+\tfrac{1}{6}\theta^4+\ldots) - Mgh\,(\tfrac{1}{2}\theta^2 - \tfrac{1}{24}\theta^4+\ldots)$$

$$= \tfrac{1}{2}\theta^2\left[\frac{(Cn)^2}{4A} - Mgh\right] + \tfrac{1}{48}\theta^4\left[\frac{(Cn)^2}{A} + 2Mgh\right] + \ldots .$$

Thus the vertical position is stable if $(Cn)^2 > 4AMgh$ and unstable if $(Cn)^2 < 4AMgh$; but, if $(Cn)^2 = 4AMgh$, $(K+V)$ is still a minimum, because $\left[(Cn)^2/A + 2Mgh\right]$ is necessarily positive. Thus *the limiting case is really stable*, in contradiction to the statement made by Routh (*loc. cit.*, p. 66) on the ground that his determinantal equation had non-linear invariant-factors; this result was first corrected by Klein (Princeton lectures, 1896, and *Theorie des Kreisels*, Leipzig, 1898, p. 316), but the above arrangement of the proof is Prof. Love's (in the manuscript already alluded to).* What Routh's work really implies is simply that the terms retained by him are not sufficient to discriminate (in the limiting case) between stability and instability.

Practical Stability.

Let us examine the case in which T' contains only one velocity; then, for *small* values of θ, the energy-equation can be reduced to the form†

$$\dot\theta^2 = v^2 - A_1\theta^2 - A_2\theta^4 - \ldots,$$

where v is small and is the value of $\dot\theta$ when $\theta = 0$. The amplitude of the deviation from $\theta = 0$ is given by the real value of θ which gives $\dot\theta = 0$; we shall determine whether there is any such real value which is small enough to make the series for $\dot\theta^2$ convergent. If such a value of θ does exist, it will be given (according to a proposition of Weierstrass's) approximately by

---

* In my note, as originally written, a similar proof was given, but without the use of the minimum-criterion; the method of the next paragraph was employed instead.

† Assuming (as is usually the case) that $(K+V)$ is an even function of θ; of course, even if this is not true, the series would start with $(v^2 - A_1\theta^2)$, without a term in θ, for this is the condition that $\theta = 0$ may be a possible steady motion.

$$\theta^2 = -\frac{A_1}{2A_2} \pm \left(\frac{A_1^2}{4A_2^2} + \frac{v^2}{A_2}\right)^{\frac{1}{2}},$$

and, in discussing the stability of an assigned system, A_1, A_2 are definite constants, while v is capable of being chosen as small as we please. Thus we have the approximate solutions

$$\theta^2 = -\frac{A_1}{2A_2} \pm \left(\frac{A_1}{2A_2} + \frac{v^2}{A_1}\right) \quad (A_1 \neq 0),$$

and the solution we require is now seen to be

$$\theta = vA_1^{-\frac{1}{2}},$$

which is *real* provided $A_1 > 0$; and can be made as small as we please by sufficiently diminishing v, and therefore small enough to make the series for $\dot{\theta}^2$ convergent. Thus, if $A_1 > 0$, the system is theoretically stable, at any rate for path.

In the same way, if $A_1 = 0$, the system will be stable if $A_2 > 0$, for then the value of θ is approximately $v^{\frac{1}{2}}A_2^{-\frac{1}{4}}$, which is real and can be made as small as we please by diminishing v sufficiently. But, in discussing the *practical* stability of similar dynamical systems with different constants, we should measure their relative stability by comparing the values of θ in the different systems which correspond to a definite value of v, *the same for all the systems.* Let us consider in this sense the practical stability of the systems which are represented by small positive and negative values of A_1; corresponding to some of these, the ratio $(A_1^2/4A_2v^2)$ will be *small* (as v is *assigned*, and A_1 varies continuously from positive to negative). When $(A_1^2/4A_2v^2)$ is small, the approximate solution given by $\dot{\theta} = 0$ becomes

$$\theta = v^{\frac{1}{2}}A_2^{-\frac{1}{4}},$$

which is *real* if $A_2 > 0$. Hence the *practical* stability does not now depend on the sign of A_1 but on that of A_2; and, with this interpretation, we may make the following statements (in all of which "stability" means "*path*-stability" not *complete* stability):—

If the motion in the "critical case" ($A_1 = 0$) *is really stable* (*i.e.*, $A_2 > 0$), *then motions for which the critical condition is nearly satisfied are "practically stable," whether theoretically stable or unstable.*

In exactly the same way we see that—

If the motion in the "critical case" ($A_1 = 0$) *is really unstable* (*i.e.*, $A_2 < 0$), *then motions for which the critical condition is nearly satisfied are "practically unstable," whether theoretically stable or unstable.*

These theorems were contained (in substance) in this note when originally presented to the Society, but the form of statement employed was somewhat misleading, and has been modified at the suggestion of the referees; a special case of the former theorem was noticed first for the case of the top by Klein,[*] and, when working out some details about the motion of a solid of revolution through a liquid, I noticed that the same point occurred there; I was thus led to attempt to construct a general theory.

Falling away from the Steady Motion in the Unstable Case without Disturbance.

If our system is such that $A_1 < 0$, say $A_1 = -a^2$ where a is real and positive, we have the equation of motion

$$\dot{\theta}^2 = a^2\theta^2 - A_2\theta^4 + \dots,$$

assuming that $\dot{\theta} = 0$ when $\theta = 0$. If we write $x = e^{at}$, we find the differential equation

$$x\frac{d\theta}{dx} = \pm\theta\left(1 - \frac{A_2}{2a^2}\theta^2 + \dots\right),$$

in which the variables can be separated. We find one solution which vanishes for $x = 0$, of the type

$$\theta = x\,(k + lx^2 + mx^4 + \dots),$$

as the other solution proceeds in powers of $1/x$. This expression for θ vanishes for $x = 0$, *i.e.*, $t = -\infty$, and for no other real value of t; thus it is clear that after an infinite time the system falls away from the steady motion and never returns to it; or $\theta = 0$ is what Poincaré has called an *asymptotic* solution of the equation of motion.

This point has been illustrated in a number of special cases by Greenhill ("On the Stability of Orbits," *Proc. Lond. Math. Soc.*, Vol. XXII., pp. 264–305, published 1892, read 1888), who has ob-

---

[*] *American Bulletin of Math.*, 1896-7, 2nd Series, Vol. III., p. 129 (a somewhat misleading misprint is corrected on p. 292); Klein-Sommerfeld, *Theorie des Kreisels*, Leipzig, 1898, p. 316.

tained *exact* solutions. The corresponding problem for the top, which involves pseudo-elliptic functions, has been discussed by Greenhill (*Elliptic Functions*, p. 243, see also Klein-Sommerfeld); and a hydrodynamical problem is solved by Greenhill in the *American Journal of Mathematics*, Vol. xx., 1898, pp. 54–64.

Comparison with Oscillations about a Position of Equilibrium.

Since the equation we have used (that is, $\dot{\theta}^2 = v^2 - A_1\theta^2 - A_2\theta^4 - \dots$) is of the type that would present itself if the system were oscillating about a position of equilibrium instead of a state of steady motion, we can apply some of Larmor's results (*Proc. Camb. Phil. Soc.*, Vol. IV., 1883, p. 410). He finds that the period of an oscillation of amplitude θ (A_1 being small in comparison with $A_2\theta^2$) is approximately

$$\frac{1}{(2A_2)^{\frac{1}{4}}\theta}\left(F - \frac{A_1 E}{2A_2\theta^2}\right),$$

where F and E are the first and second complete elliptic integrals to modulus $1/\sqrt{2}$, so that, to three places of decimals, $F = 1{\cdot}854$ $E = 1{\cdot}351$. If we introduce the value of θ given by

$$\theta^2 = \frac{v}{A_{\frac{1}{2}}} - \frac{A_1}{2A_2},$$

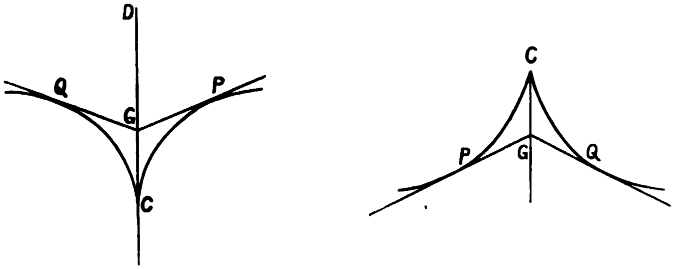
we shall have for the period the approximate value

$$\frac{(1{\cdot}854)}{(2v)^{\frac{1}{4}}A_2^{\frac{1}{4}}}\left[1 - \frac{A_1}{vA_2^{\frac{1}{2}}}({\cdot}114)\right];$$

so that the vibrations will be very slow.

Larmor's results will enable us to realize more easily the way in which a theoretical instability may be practically stable. For all systems with the same equation of motion may be regarded as dynamically the same; and the one with the above equation which is most readily pictured mentally is a solid of revolution resting on a horizontal table. The positions of equilibrium are found by drawing tangents from the centre of gravity to the evolute of the surface, and the position is stable or unstable according as the point of contact is above or below the centre of gravity. Now the evolute has a cusp, corresponding to the vertex of the solid, and the cases which we are at present discussing are represented by the vertical position being nearly neutral, or by the centre of gravity being on the axis, near the cusp; in fact A_1 is here proportional to the distance between the centre of gravity and the cusp.

Consider the state of affairs represented by the figure with the cusp downwards; here the position of equilibrium with GC vertical is unstable, but those given by GP, GQ are obviously stable. If the distance GC is small, the unstable position GC is protected by the two flanking stable positions GP, GQ, so that the deviation of GC from the vertical cannot be much greater than the angle PGD. Such a position may be called theoretically unstable but practically stable. Similarly, the theoretically stable but practically unstable case is represented by the second figure with the cusp upwards.



[In these figures the distance GC is enlarged for convenience of drawing.]

It will probably save misconception if I point out, once for all, that the reduction of the problem of oscillation about a state of steady motion to an oscillation about a position of equilibrium is only possible in the special case already discussed. For, although the energy-equation takes the form

$$T'+K+V = \text{const.},$$

whatever be the number of velocities which appear in T', yet it is impossible to obtain correctly any of the other equations of motion from this form of the energies. For, to do so, we must return to the original Lagrangian function and modify it in Routh's way (*Stability of Motion*, 1877, p. 60, Art. 20) by "ignoring" the coordinates corresponding to the constant momenta.

It will now be clear that the condition that $(K+V)$ should be a minimum of stability of a state of steady motion may not be *necessary* as well as sufficient; this in spite of the fact that the minimum condition of the potential energy is necessary for the stability of a position of equilibrium,* whatever be the number of coordinates involved.

---

* Liapunoff, *Liouville's Journal*, 5th Series, t. III., 1897, p. 332. Kneser, *Crelle's Journal*, Bd. cxv., 1895, p. 308; Bd. cxviii., 1897, p. 186. Painlevé, *Comptes Rendus*, t. cxxv., 1897, p. 1021.

The point that $(K+V)$ *may* be a maximum in stable motion is clearly brought out by an example given by Basset (*loc. cit. supra*), whose method of investigation differs somewhat from the following. The steady motion considered is that of a solid turning about a fixed point under no forces; if we use Euler's angles and eliminate $\dot\psi$ by means of $\dfrac{\partial T}{\partial\dot\psi} = H$, we can reduce T to the form

$$T'+\tfrac{1}{2}H^2/(A\cos^2\phi\sin^2\theta+B\sin^2\phi\sin^2\theta+C\cos^2\theta).$$

Thus K is a minimum when the rotation is about the A-axis, and a maximum when the rotation is about the C-axis $(A>B>C)$. Now, taking Euler's equations, we have

$$A\dot\omega_1-(B-C)\,\omega_2\omega_3 = 0, \text{ \&c.};$$

so, as usual,
$$A\omega_1^2+B\omega_2^2+C\omega_3^2 = 2T,$$
$$A^2\omega_1^2+B^2\omega_2^2+C^2\omega_3^2 = G^2,$$

where T, G are constants. We suppose that initially $\omega_3 = n$, $\omega_1 = v$, $\omega_2 = 0$, where v is small. Then we find

$$(A-B)\,A\,(\omega_1^2-v^2) = (B-C)\,C\,(\omega_3^2-n^2),$$
$$(A-B)\,B\omega_2^2 \qquad = (A-C)\,C\,(n^2-\omega_3^2).$$

It follows that, in a real motion, $n^2>\omega_3^2$, and so $v^2>\omega_1^2$; thus $(n^2-\omega_3^2)$ is of order v^2, and hence ω_2^2 is of order v^2. These facts indicate that Poinsot's polhode is a small closed curve round the end of the C-axis on the momental ellipsoid, whose linear dimensions are proportional to v. Thus the state of rotation about the C-axis is stable (at least for *path*), in spite of the fact that K is then a maximum; for by choosing v sufficiently small we can make the deviation of the disturbed path from the undisturbed path less than any assignable magnitude, however small.

In exactly the same way we can prove that the rotation about the A-axis will be stable (as it ought to be from the minimum-criterion); while that about the B-axis will not be stable. In this case K is stationary, but neither a maximum nor a minimum.

It seems possible, though I have no precise proof, that this may be capable of generalization. I have shown in another paper (p. 209 of this volume) that the roots of Routh's determinantal equation are *real* in certain cases, provided that $(K+V)$ is either a true maximum or a true minimum; but I do not think that the method can be extended so as to prove the *complete* stability.

Solid with Helicoidal Symmetry moving in an Infinite Fluid, under no Forces.

Here, with the usual notation, the kinetic energy is given by

$$2T = A(u^2+v^2)+Cw^2+P(p^2+q^2)+Rr^2+2L(up+vq)+2Nwr+K,$$

where K is constant and depends on the cyclic constants in case the solid is perforated. The complete Lagrangian function then is given by

$$L = T+\alpha w+\beta r-2K,$$

where α, β are constants and represent the linear and angular momenta due to the cyclic motion alone.

Now let us form the corresponding Hamiltonian function H; then, if

$$\xi = \frac{\partial L}{\partial u}, \text{ \&c.,} \quad \lambda = \frac{\partial L}{\partial p}, \text{ \&c.,}$$

we have

$$\begin{aligned} 2H &= 2(u\xi+\ldots+\lambda p+\ldots)-2L \\ &= u\xi+v\eta+w(\xi-\alpha)+\lambda p+\mu q+(\nu-\beta)r \\ &= \frac{1}{AP-L^2}\left[P(\xi^2+\eta^2)-2L(\lambda\xi+\mu\eta)+A(\lambda^2+\mu^2)\right] \\ &\quad + \frac{1}{CR-N^2}\left[R(\zeta-\alpha)^2-2N(\zeta-\alpha)(\nu-\beta)+C(\nu-\beta)^2\right]. \end{aligned}$$

For brevity it will be convenient to denote the coefficients in this expression for $2H$ by A_1, P_1, ..., so that

$$A_1 = A/(AP-L^2), \quad P_1 = P/(AP-L^2), \quad L_1 = L/(AP-L^2),$$
$$C_1 = C/(CR-N^2), \quad R_1 = R/(CR-N^2), \quad N_1 = N/(CR-N^2).$$

The equations of motion are now given by

$$\dot{\xi} = \eta\frac{\partial H}{\partial \nu}-\zeta\frac{\partial H}{\partial \mu}, \text{ \&c.,}$$

$$\dot{\lambda} = \eta\frac{\partial H}{\partial \zeta}-\zeta\frac{\partial H}{\partial \eta}+\mu\frac{\partial H}{\partial \nu}-\nu\frac{\partial H}{\partial \mu}, \text{ \&c.,}$$

which can be verified by using Kirchhoff's equations and substituting from the known relations*

$$u = \frac{\partial H}{\partial \xi}, \text{ \&c.,} \quad p = \frac{\partial H}{\partial \lambda}, \text{ \&c.}$$

These equations of motion can also be obtained from the general Hamiltonian equations of motion, which may be written

$$\delta H = \Sigma\,(\dot{\theta}\,\delta\phi - \dot{\phi}\,\delta\theta),$$

where θ is a typical coordinate, and ϕ the corresponding momentum.

From the equations of motion (or from first principles) it follows that ξ, η, ζ is a vector fixed in magnitude and direction; and let us take this direction as an axis from which to measure polar coordinates, so that we write

$$\xi^2+\eta^2+\zeta^2 = F^2,$$

and

$$\zeta = F\cos\theta.$$

Again, from the equations of motion, we have

$$\lambda\xi+\mu\eta+\nu\zeta = \text{const.} = FG, \text{ say,}$$

and

$$H = \text{const.}$$

Now take the third of each group of the equations, and we find

$$\dot{\zeta} = \xi\,(A_1\mu - L_1\eta) - \eta\,(A_1\lambda - L_1\xi) = A_1\,(\mu\xi - \lambda\eta),$$

$$\dot{\nu} = \xi\,(P_1\eta - L_1\mu) - \eta\,(P_1\xi - L_1\lambda) + \lambda\,(A_1\mu - L_1\eta) - \mu\,(A_1\lambda - L_1\xi) = 0.$$

Hence

$$\nu = \text{const.},$$

as proved by Clebsch (*loc. cit.*, p. 249). We can now find an equation for θ; for we have

$$\xi^2+\eta^2 = F^2\sin^2\theta,$$

$$\lambda\xi+\mu\eta = F\,(G-\nu\cos\theta),$$

and so

$$(\lambda^2+\mu^2)(\xi^2+\eta^2) = (\lambda\xi+\mu\eta)^2 + (\lambda\eta-\mu\xi)^2$$

$$= F^2\,(G-\nu\cos\theta)^2 + (\dot{\zeta}/A_1)^2,$$

or, since

$$\dot{\zeta} = -F\dot{\theta}\sin\theta,$$

we have

$$\lambda^2+\mu^2 = (G-\nu\cos\theta)^2/\sin^2\theta + \dot{\theta}^2/A_1^2.$$

---

[*] These are known from the familiar relations connecting the Hamiltonian and Lagrangian functions. See also Clebsch, *Math. Ann.*, Bd. III., 1871, p. 238, § 2.

Thus, substituting in H,

$$2H = P_1 F^2 \sin^2\theta - 2L_1 F(G-\nu\cos\theta) + A_1(G-\nu\cos\theta)^2/\sin^2\theta$$
$$+\dot\theta^2/A_1 + R_1(F\cos\theta-\alpha)^2 - 2N_1(\nu-\beta)(F\cos\theta-\alpha) + G(\nu-\beta)^2.$$

This equation is essentially the same as that found by Miss Fawcett,[*] who has effected the reduction to elliptic integrals. We shall now apply this equation to the consideration of the stability of our solid when screwing along its axis through the fluid.

In this steady motion $\theta = 0,\ \dot\theta = 0,$

and so $G = \nu.$

Let the disturbance be effected by making $\dot\theta = v$, when $\theta = 0$; then, expanding in powers of θ,

$$(\dot\theta^2 - v^2)/A_1$$
$$= -\left[P_1 F^2 - L_1 F\nu + \tfrac{1}{4}A_1\nu^2 + N_1 F(\nu-\beta) - R_1 F(F-\alpha)\right](\theta^2 - \tfrac{1}{12}\theta^4)$$
$$-\tfrac{1}{4}(-P_1F^2 + \tfrac{1}{4}A_1\nu^2 + R_1F^2)\theta^4 + \text{higher powers of } \theta.$$

Hence, according to the general theory already explained, the theoretical conditions for stability are that

$$\tfrac{1}{4}A_1\nu^2 + F\left[P_1F - L_1\nu + N_1(\nu-\beta) - R_1(F-\alpha)\right] > 0,$$

and, in case this should be zero,

$$\tfrac{1}{4}A_1\nu^2 + (R_1 - P_1)F^2 > 0.$$

The first of these is the one given by Miss Fawcett (p. 250, *loc. cit.*, *supra*) who investigates it by means of the method of small oscillations; in the special case of a solid of revolution without cyclic motion, we have

$$\alpha = 0,\quad \beta = 0,\quad L = 0,\quad N = 0,$$

and thus

$$A_1 = 1/P,\quad P_1 = 1/A,\quad L_1 = 0,$$
$$C_1 = 1/R,\quad R_1 = 1/C,\quad N_1 = 0;$$

so the first condition reduces to

$$\tfrac{1}{4}\nu^2/P + F^2(1/A - 1/C) > 0,$$

---

[*] *Quart. Jour. of Math.*, Vol. xxvi., 1893, p. 242; for Miss Fawcett's purpose it was not necessary, as here, to express the precise value of $\dot\theta$, so much as to find the general *form* for $\dot\theta$.

as was found by Greenhill;[*] while the second is

$$\tfrac{1}{4}\nu^2/P+F^2(1/C-1/A)>0.$$

But the second is only to be used in case the first is zero, and so is always positive; or the critical case is now stable, as in the top-problem.

For *practical* stability, if the quantity

$$\tfrac{1}{4}A_1\nu^2+F\left[P_1F-L_1\nu+N_1(\nu-\beta)-R_1(F-\alpha)\right]$$

be small, of the same order as v^{1+p} $(p>0)$, the stability turns on the sign of

$$\tfrac{1}{4}A_1\nu^2+(R_1-P_1)F^2.$$

If the second quantity is positive, the steady motion is practically stable, whatever be the sign of the first, provided it be small; while, if the second be negative, the steady motion is practically unstable in like manner.

In the case of the unperforated solid of revolution, since the critical case has been proved to be stable, the theoretically unstable motions which are *near* the critical state will be practically stable.

Greenhill has considered at length (*American Journal of Mathematics*, Vol. xx., 1898, p. 1) the discussion of the motion of the unperforated solid of revolution by means of elliptic functions; in particular (pp. 54–64) he considers the falling away of the solid from the steady motion in case the condition for stability is not satisfied, and shows that, if no disturbance is given, the motion is pseudo-elliptic.

In the case of the top Klein determines the limiting angle of deviation from the vertical by means of diagrams; this method has the advantage of exactness, but in the problem in hand there are a great many alternative possibilities which tend to complicate the investigation. We shall indicate the method briefly without going into full details. Take the equation giving $\dot{\theta}$ in terms of θ, and write

$$\dot{\theta}=0,\quad \cos\theta=1-x,\quad v=y;$$

then, for a given value of y, we have to find that value of x which lies between 0 and 2. This value of x will fix the extreme value of the deviation from the steady motion; and so we should trace the cubic curve

$$y^2=2mx+nx^2+lx/(2-x),$$

---

[*] *Quart. Jour. of Math.*, Vol. xvi., 1879, p. 256; *Encyc. Brit.*, 1881, "Hydromechanics," pp. 456, 457.

where $$l = A_1^2\nu^2, \quad n = A_1(R_1-P_1)F^2,$$

$$m = FA_1\left[P_1F - L_1\nu + N_1(\nu-\beta) - R_1(F-\alpha)\right].$$

In Klein's case the quantity n is zero—a fact which considerably reduces the number of types.* There is no difficulty in tracing the curve for any particular case; one device is, perhaps, worth mentioning. Since $l > 0$, it follows that $(y^2-2mx-nx^2)$ and $x/(2-x)$ are of the same sign; hence the plane is to be divided into regions by the conic $y^2-(2mx+nx^2)=0$ and the lines $x=0$, $x=2$; then the curve is either outside the conic and between the lines, or inside the conic and outside the lines.

In this way we find precisely the same results as those already indicated by the use of infinite series; this provides a check on the accuracy of the former work.

The Distribution of Velocity and the Forms of the Stream Lines due to the Motion of an Ellipsoid in Fluid, Frictionless or Viscous. By THOMAS STUART.

Communicated by Dr. J. LARMOR, February 14th, 1901. Received, in revised form, May 17th, 1901.

1. In the *Quarterly Journal of Mathematics*, Vol. XXVI., pp. 70–74, D. Edwardes has investigated the motion due to an ellipsoid which is rotating with a small angular velocity ω round a principal axis in an infinite mass of incompressible viscous liquid, and by an ingenious, though indirect, method he deduces the component velocities of the fluid at any point, and hence the whole circumstances of the motion.

We begin by developing a more direct method of treating this problem, by analogy with Oberbeck's solution (*Borchardt*, Vol. LXXXI., p. 62) for an ellipsoid moving parallel to a principal axis, and the corresponding solutions in a perfect liquid. The results are readily extended to rotation round any axis through the centre of the ellipsoid.

---

* There are three types given by $n = 0$ (one, for which $l+4m = 0$, is not drawn by Klein), and I have found twelve others; the discriminating quantities are the signs of $(l+4m)$, m, n, $(n-m)$, $(n+m)$.

Let the semiaxes of the ellipsoid be a, b, c, and let $2\pi abc\Omega$ denote the gravitational potential at an external point of this ellipsoid, supposed of unity density, so that

$$\Omega = \tfrac{1}{2}\left(A_\lambda x^2 + B_\lambda y^2 + C_\lambda z^2\right) - H_\lambda, \tag{1}$$

where

$$A_\lambda = \int_\lambda^\infty \frac{d\psi}{(a^2+\psi)\,\Delta_\psi}, \quad B_\lambda = \int_\lambda^\infty \frac{d\psi}{(b^2+\psi)\,\Delta_\psi}, \quad C_\lambda = \int_\lambda^\infty \frac{d\psi}{(c^2+\psi)\,\Delta_\psi},$$

and

$$H_\lambda = \tfrac{1}{2}\int_\lambda^\infty \frac{d\psi}{\Delta_\psi},$$

Δ_ψ denoting $\sqrt{(a^2+\psi)(b^2+\psi)(c^2+\psi)}$.

When this ellipsoid moves in a viscous fluid, parallel to the axis of x, with a constant velocity, the pressure at any point is of the form $\alpha_0 \dfrac{dH_\lambda}{dx} + \beta_0$, where α_0 and β_0 are constants (Basset, *Hydrodynamics*, Vol. II., p. 274). If a sphere is rotating round an axis through its centre in a viscous fluid, the motion set up is such that the pressure at all points of the fluid is the same and equal to the pressure at infinity. Again, in a perfect liquid, the velocity potentials for motion parallel to and rotation round the axis of x are respectively proportional to $\dfrac{d\Omega}{dx}$ and $y\dfrac{d\Omega}{dz} - z\dfrac{d\Omega}{dy}$. This suggests that when $\dfrac{d}{dx}$ of any function occurs in the linear motion parallel to x we may have $y\dfrac{d}{dz} - z\dfrac{d}{dy}$ of the same function in the angular motion round the same axis.

The equations of viscous motion are, neglecting the products and squares of the velocities,

$$\left.\begin{aligned} \nabla^2 u &= \frac{1}{\mu}\frac{d\Pi}{dx} \\ \nabla^2 v &= \frac{1}{\mu}\frac{d\Pi}{dy} \\ \nabla^2 w &= \frac{1}{\mu}\frac{d\Pi}{dz} \end{aligned}\right\}, \tag{2}$$

and the equation of continuity is

$$\frac{du}{dx}+\frac{dv}{dy}+\frac{dw}{dz}=0.$$

Thus $$\nabla^2\Pi = 0,$$

and in the problem of rotation round the axis of x we may try for the pressure the solution

$$\Pi = \Pi_0+K_0\left(y\frac{dH_\lambda}{dz}-z\frac{dH_\lambda}{dy}\right),$$

where Π_0 is the pressure at infinity and K_0 is a constant. Now

$$y\frac{dH_\lambda}{dz}-z\frac{dH_\lambda}{dy}=\frac{p_1^2yz}{\Delta_\lambda}\left(\frac{1}{c^2+\lambda}-\frac{1}{b^2+\lambda}\right)=(b^2-c^2)\frac{p_1^2yz}{(b^2+\lambda)(c^2+\lambda)}$$

$$=-\tfrac{1}{2}(b^2-c^2)\frac{d^2\Omega}{dy\,dz}.$$

Hence $$\Pi = \Pi_0-\tfrac{1}{2}K_0(b^2-c^2)\frac{d^2\Omega}{dy\,dz}.$$

The second term vanishes if the ellipsoid becomes a sphere, and hence Π would be constant throughout the fluid, as it should be, in agreement with the result above stated.

Expressing our assumption in the form

$$\Pi = \Pi_0+\mu K\frac{d^2\Omega}{dy\,dz},$$

where K is a constant, we have

$$\left.\begin{aligned}\nabla^2 u &= K\frac{d^3\Omega}{dx\,dy\,dz}\\ \nabla^2 v &= K\frac{d^3\Omega}{dy^2\,dz}\\ \nabla^2 w &= K\frac{d^3\Omega}{dy\,dz^2}\end{aligned}\right\}. \qquad (3)$$

The particular solutions, involving Ω, of this system of equations, are evidently

$$u = \alpha x\frac{d^2\Omega}{dy\,dz}+\beta y\frac{d^2\Omega}{dz\,dx}+\gamma z\frac{d^2\Omega}{dx\,dy}, \qquad (4)$$

$$v = \alpha_1 z\frac{d^2\Omega}{dy^2}+\beta_1 y\frac{d^2\Omega}{dy\,dz}, \qquad (5)$$

$$w = \alpha_2 z\frac{d^2\Omega}{dy\,dz}+\beta_2 y\frac{d^2\Omega}{dz^2}, \qquad (6)$$

where $$\alpha+\beta+\gamma = \alpha_1+\beta_1 = \alpha_2+\beta_2 = \tfrac{1}{2}K. \tag{7}$$

To these values of u, v, w we must add terms from the solutions of

$$\nabla^2 u' = 0, \quad \nabla^2 v' = 0, \quad \nabla^2 w' = 0,$$

which make the results suit the surface conditions $u = 0$, $v = -\omega_1 z$, $w = \omega_1 y$. The value of u can satisfy the surface conditions without any addition, but we add to the right-hand sides of (5) and (6) the terms $\gamma_1 \frac{d\Omega}{dz}$ and $\gamma_2 \frac{d\Omega}{dy}$ respectively, which satisfy $\nabla^2 v' = 0$, $\nabla^2 w' = 0$, and, at the surface, take the values suitable for the boundary conditions.

The complete values of u, v, w then are

$$u = \alpha x \frac{d^2\Omega}{dy\,dz} + \beta y \frac{d^2\Omega}{dz\,dx} + \gamma z \frac{d^2\Omega}{dx\,dy},$$

$$v = \alpha_1 z \frac{d^2\Omega}{dy^2} + \beta_1 y \frac{d^2\Omega}{dy\,dz} + \gamma_1 \frac{d\Omega}{dz},$$

$$w = \alpha_2 z \frac{d^2\Omega}{dy\,dz} + \beta_2 y \frac{d^2\Omega}{dz^2} + \gamma_1 \frac{d\Omega}{dy}.$$

The condition $u = 0$ at the surface gives

$$a^2\alpha + b^2\beta + c^2\gamma = 0. \tag{8}$$

Again, $v = -\omega z$ at the surface gives

$$(\alpha_1 B + \gamma_1 C) - \frac{2p^2y^3}{ab^3c}\left(\frac{\alpha_1}{b^2} + \frac{\beta_1}{c^2}\right) = 0,$$

and this requires $$\left.\begin{aligned} \frac{\alpha_1}{b^2} + \frac{\beta_1}{c^2} &= 0 \\ \alpha_1 B + \gamma_1 C &= -\omega_1 \end{aligned}\right\}. \tag{9}$$

Similarly, $w = \omega_1 y$ at the surface requires

$$\left.\begin{aligned} \frac{\alpha_2}{b^2} + \frac{\beta_2}{c^2} &= 0 \\ \beta_2 C + \gamma_2 B &= \omega_1 \end{aligned}\right\}. \tag{10}$$

From (7), (9), and (10) we get

$$\alpha_1 = \alpha_2 = \frac{Kb^2}{2(b^2-c^2)}, \quad \beta_1 = \beta_2 = \frac{-Kc^2}{2(b^2-c^2)};$$

$$\gamma_1 = -\left[\frac{\omega_1}{C} + \frac{Kb^2B}{2C(b^2-c^2)}\right], \quad \gamma_2 = \frac{\omega_1}{B} + \frac{Kc^2C}{2B(b^2-c^2)}.$$

The equation of continuity requires

$$(a+\beta_1+\gamma_1+a_2+\gamma_2)\frac{d^2\Omega}{dy\,dz}+y\frac{d}{dz}\left(\beta\frac{d^2\Omega}{dx^2}+\beta_1\frac{d^2\Omega}{dy^2}+\beta_2\frac{d^2\Omega}{dz^2}\right)$$

$$+z\frac{d}{dy}\left(y\frac{d^2\Omega}{dx^2}+a_1\frac{d^2\Omega}{dy^2}+a_2\frac{d^2\Omega}{dz^2}\right)$$

$$+ax\frac{d^3\Omega}{dx\,dy\,dz}\equiv 0.$$

But $\beta_1=\beta_2$ and $a_1=a_2$; hence

$$(a+a_1+\beta_1+\gamma_1+\gamma_2)\frac{d^2\Omega}{dy\,dz}+y(\beta-\beta_1)\frac{d^3\Omega}{dx^2\,dz}+z(\gamma-a_1)\frac{d^3\Omega}{dx^2\,dy}$$

$$+ax\frac{d^3\Omega}{dx\,dy\,dz}\equiv 0.$$

This requires

$$a=0,\quad a_1+\beta_1+\gamma_1+\gamma_2=0,\quad \beta=\beta_1,\quad \gamma=a_1. \qquad (11)$$

Now, if $a=0$ and $\beta=\beta_1$, we have, from (8),

$$b^2\beta_1+c^2\gamma=0,$$

and, from (9), $\quad b^2\beta_1+c^2a_1=0,$

and hence $\quad \gamma=a_1.$

Hence all the equations are consistent.

From (11), we have $\quad \gamma_1+\gamma_2=-\tfrac{1}{2}K,$

and, substituting values of γ_1 and γ_2 found above, we get

$$K=-\frac{2\omega_1(b^2-c^2)}{b^2B+c^2C}.$$

Hence $\quad \beta=\beta_1=\beta_2=-\gamma_1=\dfrac{\omega_1c^2}{b^2B+c^2C}$

and $\quad \gamma=a_1=a_2=-\gamma_2=\dfrac{-\omega_1b^2}{b^2B+c^2C}.$

Therefore the component velocities are given by

$$u=\sigma_1\left[c^2y\frac{d^2\Omega}{dz\,dx}-b^2z\frac{d^2\Omega}{dx\,dy}\right],$$

$$v=\sigma_1\left[c^2y\frac{d^2\Omega}{dy\,dz}-b^2z\frac{d^2\Omega}{dy^2}-c^2\frac{d\Omega}{dz}\right],$$

$$w=\sigma_1\left[c^2y\frac{d^2\Omega}{dz^2}-b^2z\frac{d^2\Omega}{dy\,dz}+b^2\frac{d\Omega}{dy}\right],$$

where
$$\sigma_1 = \frac{\omega_1}{b^2B+c^2C};$$

or by the following scheme, showing clearly the analogy with Oberbeck's solution for motion parallel to a principal axis :—

$$\left.\begin{aligned} u &= \sigma_1 \frac{d\phi_1}{dx} \\ v &= \sigma_1 \left[\frac{d\phi_1}{dy} - 2c^2 \frac{d\Omega}{dz}\right] \\ w &= \sigma_1 \left[\frac{d\phi_1}{dz} + 2b^2 \frac{d\Omega}{dy}\right] \end{aligned}\right\}, \qquad (12)$$

where ϕ_1 stands for $\left(c^2y\frac{d\Omega}{dz} - b^2z\frac{d\Omega}{dy}\right)$,

and the mean pressure is given by

$$\Pi = \Pi_0 - 2\mu\sigma_1 (b^2-c^2) \frac{d^2\Omega}{dy\,dz}.$$

We now proceed to the general case of rotation about any axis. Let u_1, u_2, u_3 denote the component velocities of the fluid parallel to the axis of x, when the ellipsoid is rotating round the axes of x, y, z, with angular velocities $\omega_1, \omega_2, \omega_3$ respectively; let v_1, v_2, v_3 and w_1, w_2, w_3 have similar meanings. Then u_1, v_1, w_1 have the values given by (12), and satisfy the differential equations

$$\begin{aligned} \nabla^2 u_1 &= -2\sigma_1 (b^2-c^2) \frac{d^3\Omega}{dx\,dy\,dz}, \\ \nabla^2 v_1 &= -2\sigma_1 (b^2-c^2) \frac{d^3\Omega}{dy^2\,dz}, \\ \nabla^2 w_1 &= -2\sigma_1 (b^2-c^2) \frac{d^3\Omega}{dy\,dz^2}, \end{aligned}$$

and the surface conditions $u_1 = 0$, $v_1 = -\omega_1 z$, $w_1 = \omega_1 y$.

Similarly, the solutions of

$$\begin{aligned} \nabla^2 u_2 &= -2\sigma_2 (c^2-a^2) \frac{d^3\Omega}{dz\,dx^2}, \\ \nabla^2 v_2 &= -2\sigma_2 (c^2-a^2) \frac{d^3\Omega}{dx\,dy\,dz}, \\ \nabla^2 w_2 &= -2\sigma_2 (c^2-a^2) \frac{d^3\Omega}{dz^2\,dx}, \end{aligned}$$

where
$$\sigma_2 = \frac{\omega_2}{c^2C + a^2A},$$

subject to the conditions $u_2 = \omega_2 z$, $v_2 = 0$, $w_2 = -\omega_2 x$, are

$$u_2 = \sigma_2\left[\frac{d\phi_1}{dx} + 2c^2\frac{d\Omega}{dy}\right],$$

$$v_2 = \sigma_2\frac{d\phi_2}{dy},$$

$$w_2 = \sigma_2\left[\frac{d\phi_2}{dz} - 2a^2\frac{d\Omega}{dx}\right],$$

where ϕ_2 stands for
$$\left(a^2z\frac{d\Omega}{dx} - c^2x\frac{d\Omega}{dz}\right);$$

and the solutions of similar differential equations for u_3, v_3, w_3, subject to the surface conditions $u_3 = -\omega_3 y$, $v_3 = \omega_3 x$, $w_3 = 0$, are

$$u_3 = \sigma_3\left[\frac{d\phi_3}{dx} - 2b^2\frac{d\Omega}{dy}\right],$$

$$v_3 = \sigma_3\left[\frac{d\phi_3}{dy} + 2a^2\frac{d\Omega}{dx}\right],$$

$$w_3 = \sigma_3\frac{d\phi_3}{dz},$$

where
$$\phi_3 = \left(b^2x\frac{d\Omega}{dy} - a^2y\frac{d\Omega}{dx}\right)$$

and
$$\sigma_3 = \frac{\omega_3}{a^2A + b^2B}.$$

When the ellipsoid is rotating round an axis through the centre of the ellipsoid with an angular velocity ω, made up of components ω_1, ω_2, ω_3 round the principal axes, the component velocities at any point are given by the superposition of the above values; for, if

$$u = \sum_1^3 u_r, \quad v = \sum_1^3 v_r, \quad w = \sum_1^3 w_r,$$

then u, v, w satisfy the differential equations

$$\left.\begin{aligned} \nabla^2 u &= \frac{d\psi}{dx} \\ \nabla^2 v &= \frac{d\psi}{dy} \\ \nabla^2 w &= \frac{d\psi}{dz} \end{aligned}\right\}, \qquad (13)$$

where

$$\psi \equiv -2\left[\sigma_1 (b^2-c^2)\frac{d^2\Omega}{dy\,dz}+\sigma_2 (c^2-a^2)\frac{d^2\Omega}{dz\,dx}+\sigma_3 (a^2-b^2)\frac{d^2\Omega}{dx\,dy}\right],$$

and also the surface conditions

$$u=\omega_2 z-\omega_3 y,\quad v=\omega_3 x-\omega_1 z,\quad w=\omega_1 y-\omega_2 x.$$

But the equations (13) are the equations of motion, when Π has the value $\Pi_0+\mu\psi$, which is the value that was to be expected from our previous analysis. Hence we have at any point of the fluid

$$\left.\begin{aligned} u &= \frac{dU}{dx}+2\left(c^2\sigma_2\frac{d\Omega}{dz}-b^2\sigma_3\frac{d\Omega}{dy}\right)\\ v &= \frac{dU}{dy}+2\left(a^2\sigma_3\frac{d\Omega}{dx}-c^2\sigma_1\frac{d\Omega}{dz}\right)\\ w &= \frac{dU}{dz}+2\left(b^2\sigma_1\frac{d\Omega}{dy}-a^2\sigma_2\frac{d\Omega}{dx}\right)\end{aligned}\right\}, \tag{14}$$

where $U \equiv \sigma_1\phi_1+\sigma_2\phi_2+\sigma_3\phi_3.$

The components of the differential rotation ξ, η, ζ are given by

$$\xi=\sigma_1 D\Omega-a^2\frac{dX}{dx},$$

$$\eta=\sigma_2 D\Omega-b^2\frac{dX}{dy},$$

$$\zeta=\sigma_3 D\Omega-c^2\frac{dX}{dz},$$

where D denotes the operator $a^2\frac{d^2}{dx^2}+b^2\frac{d^2}{dy^2}+c^2\frac{d^2}{dz^2}$ and

$$X\equiv\sigma_1\frac{d\Omega}{dx}+\sigma_2\frac{d\Omega}{dy}+\sigma_3\frac{d\Omega}{dz}.$$

The couple that must be applied to the ellipsoid, in order to maintain the motion, can readily be found by direct integration over the ellipsoidal surface.

Letting N_1, N_2, N_3 denote the three normal stresses, and T_1, T_2, T_3

the three tangential stresses, we have

$$
\begin{aligned}
N &= -\Pi + 2\mu \frac{dw}{dz} \\
&= -\Pi_0 + 2\mu \left\{ \sigma_1 (b^2-c^2) \frac{d^2\Omega}{dy\,dz} + \sigma_2 (c^2-a^2) \frac{d^2\Omega}{dz\,dx} + \sigma_3 (a^2-b^2) \frac{d^2\Omega}{dx\,dy} \right. \\
&\qquad\qquad \left. + \frac{d^2U}{dz^2} + 2\left(b^2\sigma_1 \frac{d^2\Omega}{dy\,dz} - a^2\sigma_2 \frac{d^2\Omega}{dx\,dz} \right) \right\} \\
&= -\Pi_0 + 2\mu \left\{ \Sigma\sigma_1 (b^2-c^2) \frac{d^2\Omega}{dy\,dz} + \left[a^2 (\sigma_2 z - \sigma_3 y) \frac{d}{dx} + b^2 (\sigma_3 x - \sigma_1 z) \frac{d}{dy} \right. \right. \\
&\qquad\qquad \left. \left. + c^2 (\sigma_1 y - \sigma_2 x) \frac{d}{dz} \right] \frac{d^2\Omega}{dz^2} \right\},
\end{aligned}
$$

with similar values for N_1 and N_2. Also

$$
\begin{aligned}
T_3 &= \mu \left(\frac{dv}{dx} + \frac{du}{dy} \right) \\
&= 2\mu \left[\frac{d^2U}{dx\,dy} + a^2\sigma_3 \frac{d^2\Omega}{dx^2} + c^2\sigma_2 \frac{d^2\Omega}{dy\,dz} - b^2\sigma_3 \frac{d^2\Omega}{dy^2} - c^2\sigma_1 \frac{d^2\Omega}{dx\,dz} \right] \\
&= 2\mu \left[a^2 (\sigma_2 z - \sigma_3 y) \frac{d}{dx} + b^2 (\sigma_3 x - \sigma_1 z) \frac{d}{dy} + c^2 (\sigma_1 y - \sigma_2 x) \frac{d}{dz} \right] \frac{d^2\Omega}{dx\,dy},
\end{aligned}
$$

with similar values for T_1 and T_2.

Now, in the integral $\iint (Hy - Gz)\,dS$, where $H = lT_3 + mT_1 + nN_3$, $G =$ &c., we may neglect all terms containing products and powers of x, y, z which are of odd degree, as these terms clearly vanish in the integration from symmetry. We have

$$
\begin{aligned}
yH &= y\,(lT_3 + mT_1 + nN_3) \\
&= -\frac{pzy}{c^2+\lambda} \Pi_0 \\
&\quad + \frac{2\mu pzy}{c^2+\lambda} \left\{ \sigma_1 (b^2-c^2) \frac{d^2\Omega}{dy\,dz} + \sigma_2 (c^2-a^2) \frac{d^2\Omega}{dz\,dx} + \sigma_3 (a^2-b^2) \frac{d^2\Omega}{dx\,dy} \right\} \\
&\quad + 4\mu py \left\{ a^2 (\sigma_2 z - \sigma_3 y) \frac{d}{d\lambda} \left(\frac{d^2\Omega}{dx\,dz} \right) + b^2 (\sigma_3 x - \sigma_1 z) \frac{d}{d\lambda} \left(\frac{d^2\Omega}{dy\,dz} \right) \right. \\
&\qquad\qquad \left. + c^2 (\sigma_1 y - \sigma_2 x) \frac{d}{d\lambda} \left(\frac{d^2\Omega}{dz^2} \right) \right\},
\end{aligned}
$$

since
$$
l \frac{d}{dx} + m \frac{d}{dy} + n \frac{d}{dz} = 2p \frac{d}{d\lambda}.
$$

But $$\frac{d}{d\lambda}\left(\frac{d^2\Omega}{dz^2}\right) = -\frac{1}{(c^2+\lambda)\,\Delta_\lambda} - \frac{2z^2}{(c^2+\lambda)\,\Delta_\lambda} + \frac{p^2z^2}{(c^2+\lambda)^2\,\Delta_\lambda}\left[\frac{1}{a^2+\lambda}+\frac{1}{b^2+\lambda}+\frac{3}{c^2+\lambda}\right]$$

and

$$\frac{d}{d\lambda}\left(\frac{d^2\Omega}{dy\,dz}\right) = \frac{yz}{(b^2+\lambda)(c^2+\lambda)\,\Delta_\lambda}\left[-2+p^2\left(\frac{1}{a^2+\lambda}+\frac{2}{b^2+\lambda}+\frac{2}{c^2+\lambda}\right)\right],$$

with similar values for the other derivatives with regard to λ.

Retaining only the even powers and products, we have

$$[yH]_{\lambda=0} = \frac{-4\mu p_0^3\sigma_1 y^2z^2}{ab^3c^3}\left(\frac{b^2-c^2}{c^2}\right) + 4\mu p_0 y\left[c^2\sigma_1 y\frac{d}{d\lambda}\left(\frac{d^2\Omega}{dz^2}\right) - b^2\sigma_1 z\frac{d}{d\lambda}\left(\frac{d^2\Omega}{dy\,dz}\right)\right]_{\lambda=0},$$

p_0 being the value of p at the surface; that is

$$[yH]_{\lambda=0} = \frac{-4\mu\sigma_1 p_0 y^2}{abc}.$$

Similarly, $$[zG]_{\lambda=0} = \frac{4\mu\sigma_1 p_0 z^2}{abc};$$

hence $$\iint (Hy-Gz)\,dS = -\frac{4\mu\sigma_1}{abc}\iint p_0(y^2+z^2)\,dS$$
$$= -\tfrac{16}{3}\pi\mu\sigma_1(b^2+c^2).$$

Thus the required couple has for its components

$$\frac{16\pi\mu\omega_1(b^2+c^2)}{3(b^2B+c^2C)},\ \&c.,\ \&c.$$

This result may also be deduced in a somewhat different manner, for we have

$$\frac{dT_2}{dx}+\frac{dT_1}{dy}+\frac{dN_3}{dz} = 0,$$

and two similar equations; hence

$$\iint (Hy-Gz)\,dS = 0,$$

the integration extending over the ellipsoid and any exterior surface, which may be taken to be a sphere whose radius is ultimately made infinite. The values of the stresses at the spherical boundary are easily found from the previous analysis by making λ very large, and on integration we find

$$\iint (Hy - Gz)\, dS \text{ over the sphere} = \tfrac{16}{3}\pi\mu\sigma_1 (b^2 + c^2).$$

Thus we get the same value for the couple as before. The usual method (though leading to correct results in this case) of writing down the limiting forms of the velocities when the distance from the origin is increased indefinitely and thence deducing the stresses by differentiation is open to objection, since the operations are not performed in their proper order and there is no *a priori* evidence to show that they are commutative.

2. The equations of the stream lines due to the steady motion of an ellipsoid in a perfect fluid, both when moving parallel to and rotating round a principal axis, have been obtained in an integrable form by Clebsch (*Crelle*, Vol. LII., pp. 103–132, and Vol. LIII., pp. 287–292). He used Cartesian coordinates in his investigation; while Mr. Herman (*Quart. Jour. of Math.*, Vol. XXIII., pp. 378–384), who considers the same two problems, and also the case when the ellipsoid is in steady motion parallel to a principal axis in a viscous fluid, uses ellipsoidal coordinates. Mr. Herman deduces, in each case, two integrable equations and one corresponding first integral.

The object of this paper is to show that by a proper combination of Cartesian and ellipsoidal coordinates we can deduce both the first integrals in every case. The case of an ellipsoid rotating round a principal axis in a viscous liquid is also treated.

With the same notation as in § 1, let A, B, C denote the values of A_λ, B_λ, C_λ respectively when λ is zero, λ denoting the positive root of the equation

$$\frac{x^2}{a^2+\lambda} + \frac{y^2}{b^2+\lambda} + \frac{z^2}{c^2+\lambda} = 1.$$

We have also
$$\frac{d\Omega}{dx} = A_\lambda x, \quad \frac{d\Omega}{dy} = B_\lambda y, \quad \frac{d\Omega}{dz} = C_\lambda z,$$

and
$$A_\lambda + B_\lambda + C_\lambda = \frac{2}{\Delta_\lambda}.$$

The velocity potential due to the motion of an ellipsoid in an infinite liquid, when moving parallel to the axis of x with velocity V, is

$$\phi = -\frac{V}{B+C} A_\lambda x$$

(Basset, *Hydrodynamics*, Vol. I., pp. 141, 142).

Hence the differential equations of the relative stream lines are

$$\frac{dx}{\frac{d\phi}{dx}-V}=\frac{dy}{\frac{d\phi}{dy}}=\frac{dz}{\frac{d\phi}{dz}},$$

that is,

$$\frac{dx}{B+C+A_\lambda-\frac{2p_1^2x^2}{(a^2+\lambda)^2\Delta_\lambda}}=\frac{dy}{\frac{-2p_1^2xy}{(a^2+\lambda)(b^2+\lambda)\Delta_\lambda}}=\frac{dz}{\frac{-2p_1^2xz}{(a^2+\lambda)(c^2+\lambda)\Delta_\lambda}},$$

where p_1 is the perpendicular from the origin on the tangent plane to the confocal whose primary semiaxis is $\sqrt{a^2+\lambda}$.

Each of the above expressions

$$\equiv\frac{\Sigma x\frac{dx}{a^2+\lambda}}{(B+C+A_\lambda)\frac{x}{a^2+\lambda}-\frac{2x}{(a^2+\lambda)\Delta_\lambda}}\equiv\frac{d\lambda}{(B+C+A_\lambda)\frac{2p_1^2x}{a^2+\lambda}-\frac{4p_1^2x}{(a^2+\lambda)\Delta_\lambda}},$$

since $$\Sigma\frac{x\,dx}{a^2+\lambda}=\frac{d\lambda}{2p_1^2}.$$

Hence

$$\frac{\frac{dy}{y}}{\frac{1}{(b^2+\lambda)\Delta_\lambda}}=\frac{\frac{dz}{z}}{\frac{1}{(c^2+\lambda)\Delta_\lambda}}=\frac{-d\lambda}{B+C+A_\lambda-\frac{2}{\Delta_\lambda}}=\frac{-d\lambda}{B+C-B_\lambda-C_\lambda}.$$

Letting θ_λ denote $B+C-B_\lambda-C_\lambda$, then, since

$$\frac{d\theta_\lambda}{d\lambda}=\left(\frac{1}{b^2+\lambda}+\frac{1}{c^2+\lambda}\right)\frac{1}{\Delta_\lambda},$$

we have $$\frac{dy}{y}+\frac{dz}{z}+\frac{1}{\theta_\lambda}\frac{d\theta_\lambda}{d\lambda}d\lambda=0.$$

Integrating, one first integral is

$$yz\left[B+C-B_\lambda-C_\lambda\right]=\text{constant},$$

that is, $$yz\int_0^\lambda\left(\frac{1}{b^2+\psi}+\frac{1}{c^2+\psi}\right)\frac{d\psi}{\Delta_\psi}=\text{constant}.$$

This is the first integral given by Mr. Herman; the present method shows that it is the product of the integrals

$$y\,e^{\int_\lambda^\infty\frac{d\lambda}{(b^2+\lambda)\Delta_\lambda\theta_\lambda}}=\text{constant},$$

$$z\,e^{\int_\lambda^\infty\frac{d\lambda}{(c^2+\lambda)\Delta_\lambda\theta_\lambda}}=\text{constant}.$$

By squaring and adding these, we get the integral that corresponds to Stokes' current function in the case of a sphere, viz.,

$$\psi = \frac{Va^3}{2r^3}(y^2+z^2).$$

The velocity potential, when the ellipsoid is rotating round Ox with angular velocity ω, is

$$\phi = \frac{\omega}{K}(B_\lambda - C_\lambda)\,yz,$$

where K denotes $A + \frac{2(b^2B-c^2C)}{b^2-c^2}$. The differential equations of the relative stream lines are

$$\frac{dx}{\frac{d\phi}{dx}} = \frac{dy}{\frac{d\phi}{dy}+\omega z} = \frac{dz}{\frac{d\phi}{dz}-\omega y},$$

that is,

$$\frac{x\,dx}{\frac{2(b^2-c^2)p_1^2x^2}{\Delta_\lambda^3}} = \frac{y\,dy}{\frac{2(b^2-c^2)p_1^2y^2}{(b^2+\lambda)^2(c^2+\lambda)\Delta_\lambda}+B_\lambda-C_\lambda+K}$$

$$= \frac{z\,dz}{\frac{2(b^2-c^2)p_1^2z^2}{(b^2+\lambda)(c^2+\lambda)^2\Delta_\lambda}+B_\lambda-C_\lambda-K}.$$

Each of these expressions

$$\equiv \frac{\Sigma\frac{x\,dx}{a^2+\lambda}}{\frac{2(b^2-c^2)}{(b^2+\lambda)(c^2+\lambda)\Delta_\lambda}+(B_\lambda-C_\lambda)\left(\frac{1}{b^2+\lambda}+\frac{1}{c^2+\lambda}\right)+K\left(\frac{1}{b^2+\lambda}-\frac{1}{c^2+\lambda}\right)}$$

$$\equiv \frac{d\lambda}{\frac{2p_1^2}{(b^2+\lambda)(c^2+\lambda)}\left\{(b^2-c^2)\left(\frac{2}{\Delta_\lambda}-K\right)+(b^2+c^2+2\lambda)(B_\lambda-C_\lambda)\right\}}.$$

Denoting $(b^2-c^2)\left(\frac{2}{\Delta_\lambda}-K\right)+(b^2+c^2+2\lambda)(B_\lambda-C_\lambda)$ by G_λ, we have

$$\frac{dx}{x} = \frac{(b^2-c^2)\,d\lambda}{(a^2+\lambda)\Delta_\lambda G_\lambda}.$$

Thus

$$xe^{-\int_\lambda^\infty\frac{(b^2-c^2)d\lambda}{(a^2+\lambda)\Delta_\lambda G_\lambda}} = \text{constant}$$

is one first integral. A second integral cannot readily be found directly; but, observing that at a great distance from the origin the stream lines are circles, being the intersection of the planes $x =$ constant with spheres having the origin for centre, we are led to assume as another integral

$$x^2\theta(\lambda)+y^2\phi(\lambda)+z^2\psi(\lambda) = \text{constant},$$

where θ, ϕ, and ψ are unknown functions of λ.

To justify this assumption, we must have

$$2\left[x\theta(\lambda)\,dx+y\phi(\lambda)\,dy+z\psi(\lambda)\,dz\right] \\ +\left[x^2\theta'(\lambda)+y^2\phi'(\lambda)+z^2\psi'(\lambda)\right]d\lambda \equiv 0,$$

when dx, dy, dz, $d\lambda$ have the ratios given by the differential equations above.

Remembering that

$$\frac{1}{p_1^2}=\frac{x^2}{(a^2+\lambda)^2}+\frac{y^2}{(b^2+\lambda)^2}+\frac{z^2}{(c^2+\lambda)^2},$$

we get

$$\frac{2\theta(\lambda)\,x^2(b^2-c^2)}{\Delta_\lambda^3}+\phi(\lambda)\left[\frac{2(b^2-c^2)\,y^2}{(b^2+\lambda)^2(c^2+\lambda)\,\Delta_\lambda}\right. \\ \left.+(B_\lambda-C_\lambda+K)\left(\frac{x^2}{(a^2+\lambda)^2}+\frac{y^2}{(b^2+\lambda)^2}+\frac{z^2}{(c^2+\lambda)^2}\right)\right] \\ +\psi(\lambda)\left[\frac{2(b^2-c^2)\,z^2}{(b^2+\lambda)(c^2+\lambda)^2\,\Delta_\lambda}\right. \\ \left.+(B_\lambda-C_\lambda-K)\left(\frac{x^2}{(a^2+\lambda)^2}+\frac{y^2}{(b^2+\lambda)^2}+\frac{z^2}{(c^2+\lambda)^2}\right)\right] \\ +\frac{G_\lambda}{(b^2+\lambda)(c^2+\lambda)}\left[x^2\theta'(\lambda)+y^2\phi'(\lambda)+z^2\psi'(\lambda)\right] \equiv 0.$$

Here the coefficients of x^2, y^2, z^2 must all vanish. This gives

$$\frac{(b^2+\lambda)(c^2+\lambda)}{(a^2+\lambda)^2}\left[\phi(\lambda)(B_\lambda-C_\lambda+K)+\psi(\lambda)(B_\lambda-C_\lambda-K)\right] \\ +\frac{2(b^2-c^2)\,\theta(\lambda)}{(a^2+\lambda)\,\Delta_\lambda}+\theta'(\lambda)\,G_\lambda = 0,$$

$$\frac{\phi(\lambda)}{b^2+\lambda}\left[\frac{2(b^2-c^2)}{\Delta_\lambda}+(c^2+\lambda)(B_\lambda-C_\lambda+K)\right] \\ +\frac{\psi(\lambda)(c^2+\lambda)}{b^2+\lambda}(B_\lambda-C_\lambda-K)+\phi'(\lambda)\,G_\lambda = 0,$$

$$\frac{\phi(\lambda)(b^2+\lambda)}{c^2+\lambda}\left[B_\lambda-C_\lambda+K\right]$$

$$+\frac{\psi(\lambda)}{c^2+\lambda}\left[\frac{2(b^2-c^2)}{\Delta_\lambda}+(b^2+\lambda)(B_\lambda-C_\lambda-K)\right]+\psi'(\lambda)\,G_\lambda=0.$$

Putting $\phi(\lambda)=\frac{\phi_1(\lambda)}{b^2+\lambda}$ and $\psi(\lambda)=\frac{\psi_1(\lambda)}{c^2+\lambda}$,

we easily find that the last two equations become

$$(\phi_1-\psi_1)(B_\lambda-C_\lambda-K)=\frac{d\phi_1}{d\lambda}G_\lambda,$$

$$(\phi_1-\psi_1)(B_\lambda-C_\lambda+K\;=-\frac{d\psi_1}{d\lambda}G_\lambda.$$

Adding, we obtain

$$2(B_\lambda-C_\lambda)(\phi_1-\psi_1)=\left(\frac{d\phi_1}{d\lambda}-\frac{d\psi_1}{d\lambda}\right)G_\lambda.$$

But $\frac{dG_\lambda}{d\lambda}=2(B_\lambda-C_\lambda)-\frac{b^2-c^2}{(a^2+\lambda)\,\Delta_\lambda}.$

Hence $\frac{\phi_1'-\psi_1'}{\phi_1-\psi_1}=\frac{1}{G_\lambda}\left[\frac{dG_\lambda}{d\lambda}+\frac{b^2-c^2}{(a^2+\lambda)\,\Delta_\lambda}\right].$

Integrating, we have

$$\phi_1-\psi_1=A_0\,G_\lambda e^{\int_0^\lambda\frac{(b^2-c^2)\,d\lambda}{(a^2+\lambda)\,\Delta_\lambda G_\lambda}},$$

where A_0 is an arbitrary constant. Hence

$$\frac{d\phi_1}{d\lambda}=2\,(B_\lambda-C_\lambda-K)\,H_\lambda,$$

$$\frac{d\psi_1}{d\lambda}=-2\,(B_\lambda-C_\lambda+K)\,H_\lambda,$$

where H_λ denotes $e^{\int_0^\lambda\frac{(b^2-c^2)\,d\lambda}{(a^2+\lambda)\,\Delta_\lambda G_\lambda}}$, the arbitrary constant being supposed absorbed in the integral. Hence

$$\phi_1=G_\lambda H_\lambda-2K\int_0^\lambda H\,d\lambda,$$

$$\psi_1=-\,G_\lambda H_\lambda-2K\int_0^\lambda H\,d\lambda.$$

Substituting the values of ϕ and ψ, *i.e.*, of $\dfrac{\phi_1}{b^2+\lambda}$ and $\dfrac{\psi_1}{c^2+\lambda}$, in the first equation above, we get, since

$$\frac{1}{H_\lambda}\frac{dH_\lambda}{d\lambda} = \frac{b^2-c^2}{(a^2+\lambda)\,\Delta_\lambda G_\lambda},$$

$$\frac{d\theta_\lambda}{d\lambda} + \frac{2}{H_\lambda}\frac{dH_\lambda}{d\lambda}\theta_\lambda$$

$$= \frac{1}{G_\lambda (a^2+\lambda)^2}\Big[G_\lambda H_\lambda \{(B_\lambda - C_\lambda)(b^2-c^2) - K(b^2+c^2+2\lambda)\}$$
$$+2K\{(B_\lambda - C_\lambda)(b^2+c^2+2\lambda) - K(b^2-c^2)\}\int H\,d\lambda\Big]$$

$$= \frac{1}{(a^2+\lambda)^2}\Big[H_\lambda \{(B_\lambda - C_\lambda)(b^2-c^2) - K(b^2+c^2+2\lambda)\}$$
$$+2K\left\{1 - \frac{2(b^2-c^2)}{\Delta_\lambda G_\lambda}\right\}\int H\,d\lambda\Big].$$

Hence $$\frac{d}{d\lambda}\left[H_\lambda^2\theta(\lambda)\right]$$

$$= \frac{H_\lambda^3}{(a^2+\lambda)}\Big[\{(B_\lambda - C_\lambda)(b^2-c^2) - K(b^2+c^2+2\lambda)\}$$
$$+2K\left\{\frac{H_\lambda^2}{(a^2+\lambda)^2} - \frac{2H_\lambda}{a^2+\lambda}\frac{dH_\lambda}{d\lambda}\right\}\int H\,d\lambda\Big].$$

Integrating and dividing across by H_λ^2, we get

$$\theta(\lambda) = -\frac{2K}{a^2+\lambda}\int_0^\lambda H_\lambda\,d\lambda + \frac{1}{H_\lambda^2}\int_0^\lambda \frac{H_\lambda^3}{(a^2+\lambda)^2}$$
$$\times\{(B_\lambda - C_\lambda)(b^2-c^2) + K(2a^2-b^2-c^2)\}\,d\lambda.$$

Also $$\phi(\lambda) = \frac{1}{b^2+\lambda}\left[G_\lambda H_\lambda - 2K\int_0^\lambda H\,d\lambda\right],$$

$$\psi(\lambda) = -\frac{1}{c^2+\lambda}\left[G_\lambda H_\lambda + 2K\int_0^\lambda H\,d\lambda\right].$$

Thus the second integral is

$$x^2\theta(\lambda) + y^2\phi(\lambda) + z^2\psi(\lambda) = \text{constant};$$

θ, ϕ, and ψ having the above values; and the limits of the integrals having been so chosen that when λ is indefinitely increased our second integral becomes a sphere, and when zero the ellipsoid itself.

If an ellipsoidal solid is moving parallel to the axis of x with velocity V through a viscous incompressible fluid, the component velocities at any point of the fluid are given by

$$u = \alpha\left(x\frac{dH_\lambda}{dx} - H_\lambda + \beta\frac{d^2\Omega}{dx^2}\right),$$

$$v = \alpha\left(x\frac{dH_\lambda}{dy} + \beta\frac{d^2\Omega}{dx\,dy}\right),$$

$$w = \alpha\left(x\frac{dH_\lambda}{dz} + \beta\frac{d^2\Omega}{dx\,dz}\right),$$

where $\beta = -\frac{1}{2}a^2$ and $\alpha = \dfrac{-2V}{a^2A + 2H}$.

The differential equations of the relative stream lines are

$$\frac{dx}{u-V} = \frac{dy}{v} = \frac{dz}{w}.$$

Substituting and reducing, we get

$$\frac{dx}{H_\lambda - H + \frac{a^2}{2}(A_\lambda - A) + \frac{\lambda}{(a^2+\lambda)\,\Delta_\lambda}\,\frac{p_1^2x^2}{a^2+\lambda}}$$

$$= \frac{dy}{\frac{\lambda}{(a^2+\lambda)\,\Delta_\lambda}\,\frac{p_1^2xy}{(b^2+\lambda)}} = \frac{dz}{\frac{\lambda}{(a^2+\lambda)\,\Delta_\lambda}\,\frac{p_1^2xz}{c^2+\lambda}}.$$

Each of these expressions

$$\equiv \frac{\Sigma\,\frac{x\,dx}{a^2+\lambda}}{\frac{x}{a^2+\lambda}\left[H_\lambda - H + \frac{a^2}{2}(A_\lambda - A) + \frac{\lambda}{\Delta_\lambda}\right]}$$

$$\equiv \frac{d\lambda}{\frac{2p_1^2x}{a^2+\lambda}\left[H_\lambda - H + \frac{a^2}{2}(A_\lambda - A) + \frac{\lambda}{\Delta_\lambda}\right]}.$$

Hence $\dfrac{\frac{dy}{y}}{\frac{\lambda}{(b^2+\lambda)\,\Delta^\lambda}} = \dfrac{\frac{dz}{z}}{\frac{\lambda}{(c^2+\lambda)\,\Delta_\lambda}} = \dfrac{d\lambda}{2\left[H_\lambda - H + \frac{a^2}{2}(A_\lambda - A) + \frac{\lambda}{\Delta_\lambda}\right]}$

and we have

$$\frac{dy}{y} + \frac{dz}{z} - \frac{\left(\frac{1}{b^2+\lambda} + \frac{1}{c^2+\lambda}\right)\frac{\lambda\,d\lambda}{\Delta_\lambda}}{2\left[H_\lambda - H + \frac{a^2}{2}(A_\lambda - A) + \frac{\lambda}{\Delta_\lambda}\right]} = 0.$$

Integrating gives

$$yz\left\{2\,(H_\lambda - H) + a^2\,(A_\lambda - A) + \frac{2\lambda}{\Delta_\lambda}\right\} = \text{constant},$$

that is,
$$yz\left\{\int_0^\lambda \left(\frac{a^2}{a^2+\psi}+1\right)\frac{d\psi}{\Delta_\psi} - \frac{2\lambda}{\Delta_\lambda}\right\} = \text{constant}. \tag{15}$$

Letting θ_λ denote $2\,(H_\lambda - H) + a^2\,(A_\lambda - A) + \dfrac{2\lambda}{\Delta_\lambda}$, we have also the pair of first integrals

$$y\,e^{\int_\lambda^\infty \frac{\lambda\,d\lambda}{(b^2+\lambda)\Delta_\lambda\theta_\lambda}} = \text{constant},$$

$$z\,e^{\int_\lambda^\infty \frac{\lambda\,d\lambda}{(c^2+\lambda)\Delta_\lambda\theta_\lambda}} = \text{constant}.$$

The equation (15), which assumes a simple form, is clearly the porduct of these integrals. Neither of them, however, separately admits of further reduction, unless the ellipsoid is one of revolution.

When the ellipsoid is rotating in viscous incompressible fluid, round the axis of x, with small angular velocity ω, the component velocities at any point, parallel to the principal axes of the ellipsoid, are given by (*cf.* § 1)

$$u = 2\sigma\frac{(b^2-c^2)\,p_1^2\lambda xyz}{\Delta_\lambda^3},$$

$$v = 2\sigma\frac{(b^2-c^2)\,p_1^2\lambda y^2z}{(b^2+\lambda)^2\,(c^2+\lambda)\,\Delta_\lambda} - \sigma\,(b^2B_\lambda + c^2C_\lambda)\,z,$$

$$w = 2\sigma\frac{(b^2-c^2)\,p_1^2\lambda yz^2}{(b^2+\lambda)(c^2+\lambda)^2\,\Delta_\lambda} + \sigma\,(b^2B_\lambda + c^2C_\lambda)\,y,$$

where
$$\sigma = \frac{\omega}{b^2B + c^2C}.$$

The differential equations of the stream lines, relative to the moving solid, are

$$\frac{dx}{u} = \frac{dy}{v+\omega z} = \frac{dz}{w-\omega y}.$$

that is,

$$\frac{dx}{\dfrac{2p_1^2\lambda xyz\,(b^2-c^2)}{\Delta_\lambda^3}} = \frac{dy}{\dfrac{2p_1^2\lambda y^2z\,(b^2-c^2)}{(b^2+\lambda)^2\,(c^2+\lambda)\,\Delta_\lambda} - \left(b^2B_\lambda + c^2C_\lambda - \dfrac{\omega}{\sigma}\right)z}$$

$$= \frac{dz}{\dfrac{2p_1^2\lambda yz^2\,(b^2-c^2)}{(b^2+\lambda)(c^2+\lambda)^2\,\Delta_\lambda} + \left(b^2B_\lambda + c^2C_\lambda - \dfrac{\omega}{\sigma}\right)y}.$$

Each of these expressions

$$\equiv \frac{\Sigma \dfrac{x\,dx}{a^2+\lambda}}{\dfrac{(b^2-c^2)\,yz}{(b^2+\lambda)(c^2+\lambda)}\left\{b^2B_\lambda+c^2C_\lambda-\dfrac{\omega}{\sigma}+\dfrac{2\lambda}{\Delta_\lambda}\right\}}$$

$$\equiv \frac{d\lambda}{\dfrac{2p_1^2yz\,(b^2-c^2)}{(b^2+\lambda)(c^2+\lambda)}\left\{b^2B_\lambda+c^2C_\lambda-\dfrac{\omega}{\sigma}+\dfrac{2\lambda}{\Delta_\lambda}\right\}},$$

and also $\equiv \dfrac{x\,dx+y\,dy+z\,dz}{\dfrac{2p_1^2yz\lambda\,(b^2-c^2)}{(b^2+\lambda)(c^2+\lambda)\,\Delta_\lambda}}.$

Hence, removing common factors,

$$\frac{\dfrac{dx}{x}}{\dfrac{\lambda}{(a^2+\lambda)\,\Delta_\lambda}}=\frac{x\,dx+y\,dy+z\,dz}{\dfrac{\lambda}{\Delta_\lambda}}=\frac{d\lambda}{b^2B_\lambda+c^2C_\lambda-\dfrac{\omega}{\sigma}+\dfrac{2\lambda}{\Delta_\lambda}}.$$

But $\qquad \dfrac{d}{d\lambda}\left[b^2B_\lambda+c^2C_\lambda-\dfrac{\omega}{\sigma}+\dfrac{2\lambda}{\Delta_\lambda}\right]=-\dfrac{\lambda}{(a^2+\lambda)\,\Delta_\lambda}.$

Thus one first integral is

$$x\left[b^2B_\lambda+c^2C_\lambda-\frac{\omega}{\sigma}+\frac{2\lambda}{\Delta_\lambda}\right]=\text{constant},$$

that is, $\qquad x\left\{\displaystyle\int_0^\lambda\left[\frac{b^2}{b^2+\psi}+\frac{c^2}{c^2+\psi}\right]\frac{d\psi}{\Delta_\psi}-\frac{2\lambda}{\Delta_\lambda}\right\}=\text{constant}.$

The other first integral is evidently

$$x^2+y^2+z^2+2\int_\lambda^\infty\frac{\lambda\,d\lambda}{\Delta_\lambda\left[b^2(B-B_\lambda)+c^2(C-C_\lambda)\right]-2\lambda}=\text{constant}.$$

Factorisable Twin Binomials. *By* Lt.-Col. ALLAN CUNNINGHAM, R.E., Fellow of King's College, London. Read and received February 14th, 1901.

[The author is indebted to the late Mr. Chas. E. Bickmore for advice in preparing this paper, and also to Mr. H. J. Woodall for reading the proofs.]

Notation.

All symbols used denote *integers*.

ω denotes any *odd* number, ϵ denotes any *even* number.

N denotes the number proposed for factorisation.

$\mathfrak{N}$, D denote the *Numerator* and *Denominator* of the fraction $\mathfrak{N} \div D = N$.

1. *Binomial Forms.*—The functions

$$\Phi_k = \mu X^k + \nu Y^k, \quad \Phi'_k = \mu' X'^k + \nu' Y'^k, \tag{1}$$

wherein X, Y carry the *same exponent* (k), are here called *Binomial Forms*, or (for brevity) simply *Forms*, of order k. When two Binomial Forms (Φ_k, Φ'_k) of same order (k) are (numerically) *equal*, but *not identical*, they are called *Twin Forms*.

1a. A form (ϕ_k) which is numerically $= 1$, is called a *Unit-form*[*] ($\phi_k = 1$). Twin Forms (Φ_k, Φ'_k) which are interconvertible by mere[†] multiplication by one of their Unit-forms ($\phi_k = 1$)—[*i.e.*, which are such that $\Phi'_k = \Phi_k \, . \, \phi_k$ *identically*]—are called *Automorphs*. Twin Forms (Φ_k, Φ'_k) which are *non-automorphic* are styled *Non-equivalent Forms*.

2. *Working Condition.*—The following *working condition* is assumed throughout, saving much detail, without any real loss of generality,

Each of the pairs (μ, ν), (μ, Y), (ν, X), (X, Y) is a *prime-pair*, (2)

i.e., the two members of each pair are *mutually prime*.

3. *Derivation.*—When a number N is expressed in *Twin Forms* Φ_k, Φ'_k, so that

$$N = \Phi_k = \Phi'_k,$$

---

[*] *Unit-forms* can exist only when the product $\mu\nu$ is *negative*. They are common in *quadratic* forms, *e.g.*, $3 \, . \, 9^2 - 2 \, . \, 11^2 = 1$, $5^2 - 6 \, . \, 2^2 = 1$; but less common in higher orders, *e.g.*, $47 \, . \, 2^3 - 3 \, . \, 5^3 = 1$, $43 \, . \, 2^3 - 7^3 = 1$; $3^4 - 5 \, . \, 2^4 = 1$; &c.

[†] *E.g.*, $\Phi_2 = 11^2 - 6 \, . \, 2^2$, $\Phi'_2 = 31^2 - 6 \, . \, 12^2$, &c., are *Automorphs*; for $\Phi_2 \, . \, \phi_2 = \Phi'_2$ *identically*, by the Rules of *Conformal Multiplication*, taking $\phi_2 = 5^2 - 6 \, . \, 2^2 = 1$ (see the author's paper "On Connexion of Quadratic Forms," *Proc. Lond. Math. Soc.*, Vol. XXVIII., Art. 6, 9).

where
$$\Phi_k = \mu x^k + \nu y^k, \quad \Phi_k' = \mu' x'^k + \nu' y'^k, \tag{3}$$

it will now be shown how to express it in *two* ways in the form $N = \mathfrak{N} \div D$, where $\mathfrak{N}$, D are each *Binomial Forms* of order k. This process is styled* *Derivation.*

Method i.—Suppose μ, μ' to contain the common factor μ_0, and ν, ν' to contain the common factor ν_0, so that

$$\mu = \mu_0 \cdot \mu_1, \;\; \mu' = \mu_0 \cdot \mu_1'; \quad \nu = \nu_0 \cdot \nu_1, \;\; \nu' = \nu_0 \cdot \nu_1';$$

but so that μ_0, ν_0 are a *prime-pair.* (4)

Then, by (3), (4),

$$\frac{\mu_1' x'^k - \mu_1 x^k}{\nu_0} = \frac{\nu_1 y^k - \nu_1' y'^k}{\mu_0} = \textit{integer} = D \text{ (suppose)}, \tag{5}$$

and
$$N = \frac{\mu' x'^k (\mu x^k + \nu y^k)}{\mu' x'^k} = \frac{\mu x^k (\mu' x'^k + \nu' y'^k)}{\mu x^k}$$
$$= \frac{\mu' \nu (x'y)^k - \mu \nu' (xy')^k}{\mu' x'^k - \mu x^k}$$
$$= \frac{\mu_1' \nu_1 (x'y)^k - \mu_1 \nu_1' (xy')^k}{D} = \frac{\mathfrak{N}}{D}. \tag{6}$$

Method ii.—Similarly, if μ', ν contain the common factor μ_0, and ν', μ contain the common factor ν_0, so that

$$\mu' = \mu_0 \cdot \mu_1', \;\; \nu = \mu_0 \cdot \nu_1; \quad \mu = \nu_0 \cdot \mu_1, \;\; \nu' = \nu_0 \cdot \nu_1';$$

but so that μ_0, ν_0 are a *prime-pair,* (4*a*)

then, by (3), (4*a*),

$$\frac{\mu_1' x'^k - \nu_1 y^k}{\nu_0} = \frac{\mu_1 x^k - \nu_1' y'^k}{\mu_0} = \text{integer} = D \text{ (suppose)}, \tag{5a}$$

and, by steps similar to those used in Method i,

$$N = \frac{\mu_1 \mu_1' (xx')^k - \nu_1 \nu_1' (yy')^k}{D} = \frac{\mathfrak{N}}{D}. \tag{6a}$$

Thus, it has been shown how to transform a number N when expressed in twin forms ($N = \Phi_k = \Phi_k'$), into the form $N = \mathfrak{N} \div D$ in *two* (alternative) ways; but, inasmuch as the results (5), (6) differ from (5*a*), (6*a*) only in the interchange of μx^k, νy^k, the two methods differ only in notation, and it will suffice to consider only one of them, say Method i.

---

* This process (as applied to quadratic forms only) has been described under this *same name* in the author's paper "On Connexion of Quadratic Forms," Art. 24.

4. *Lemma* (on factorisation).—If

$$N = \frac{\mathfrak{N}}{D}, \tag{7}$$

and if *also* $\mathfrak{N} = L.M$, where L, M *each* > 1, (8)

then N is hereby usually resolvable into *two* factors, (8*a*)

except only, when one of $L, M = D$, or $=$ a factor of D. (8*b*)

4a. Similarly, if $\mathfrak{N} = L_1.L_2.L_3$, where L_1, L_2, L_3 each > 1, (9)

then, N is hereby usually resolvable into *three* factors, (9*a*)

except only, when one of L_1, L_2, $L_3 = D$, or $=$ a factor of D, (9*b*)

and this procedure may obviously be extended to the case of *more than three* factors.

5. *Factorisability.*—The *chief* condition of usage of twin forms in factorisation appears to be—

The twin forms (Φ_k, Φ'_k) must be *non-equivalent*. (10)

6. *Factorisable Forms of* $\mathfrak{N}$.—In order to confine the investigation within reasonable limits, it is proposed to consider only such twin forms (Φ_k, Φ'_k) as are so related as to yield the *simplest* factorisable form of the numerator $\mathfrak{N}$ of the *derived form* $(\mathfrak{N} \div D)$ obtained for N by Art. **3.** These may be arranged in *six* classes, defined by the relations between the coefficients (μ, ν, μ', ν'), styled as follows:—

Φ_k, Φ'_k are *Isomorphs** when $\mu = \mu'$, $\nu = \nu'$; *Antimorphs** when $\mu = \mu'$, $\nu = -\nu'$.

Φ_k, Φ'_k are *Conformals** when $\mu\nu = \mu'\nu'$; *Anti-conformals** when $\mu\nu = -\mu'\nu'$.

Φ_k, Φ'_k are *Quasi-conformals*† when $\dfrac{\mu\nu'}{\mu'\nu} = \left(\dfrac{n}{m}\right)^k$;

Anti-quasi-conformals† when $\dfrac{\mu\nu'}{\mu'\nu} = -\left(\dfrac{n}{m}\right)^k$.

These will be found to lead to certain forms of $\mathfrak{N}$ which may be *all* included in the general type

---

* This *corresponds* to the nomenclature originally suggested for *quadratic forms* in the author's paper on "Connexion of Quadratic Forms."

† New terms suggested by the previous terms *.

$$\mathfrak{N} = X^k - j \, . \, Y^k, \quad \text{where } j = \pm 1, \tag{11}$$

which is well known to be *always* (algebraically) factorisable, except when $j = -1$, and $k = 2^\epsilon$ $(\epsilon > 0)$.

7. *Isomorphs and Antimorphs* (Φ_k, Φ'_k).—These are the simplest *general* forms, leading to the simplest factorisable form (11) of $\mathfrak{N}$. They are defined by writing in Art. **3**,

$$\mu = \mu' = \mu_0, \quad \nu = j\nu' = \nu_0; \quad \text{where } j = \pm 1, \tag{12}$$

giving

$$\mu_1 = \mu'_1 = 1, \quad \nu_1 = 1, \quad \nu'_1 = j = \pm 1, \tag{12a}$$

$$\Phi_k = \mu_0 x^k + \nu_0 y^k, \quad \Phi'_k = \mu_0 x'^k + j\nu_0 y'^k; \quad [N = \Phi_k = \Phi'_k], \tag{13}$$

$$D = \frac{x'^k - x^k}{\nu_0} = \frac{y^k - jy'^k}{\mu_0} = \textit{integer}, \tag{14}$$

$$\mathfrak{N} = (x'y)^k - j\,(xy')^k, \tag{15}$$

which is of the *general* form required (11).

It is proposed to consider in detail only the simpler, and more interesting, forms given by $k = 2$, $j = \pm 1$, and by $k = 3$, $j = -1$ (Arts. **8**, **9**, **10**).

8. *Isomorph Quadratics* (Φ_2, Φ'_2).—Take

$$k = 2\kappa \text{ (any } \textit{even} \text{ number)}, \; j = +1, \tag{16}$$

giving

$$\Phi_{2\kappa} = \mu_0 x^{2\kappa} + \nu_0 y^{2\kappa}, \quad \Phi'_{2\kappa} = \mu_0 x'^{2\kappa} + \nu_0 y'^{2\kappa}, \quad [N = \Phi_{2\kappa} = \Phi'_{2\kappa}], \tag{17}$$

$$D = \frac{x'^{2\kappa} - x^{2\kappa}}{\nu_0} = \frac{y^{2\kappa} - y'^{2\kappa}}{\mu_0} = \text{integer}, \tag{18}$$

$$\mathfrak{N} = (x'y)^{2\kappa} - (xy')^{2\kappa}, \quad \textit{a difference of squares.} \tag{19}$$

Here the twin forms $(\Phi_{2\kappa}, \Phi'_{2\kappa})$ are *isomorph quadratic* forms, a case *known** to be always factorisable (when $\Phi_{2\kappa}$, $\Phi'_{2\kappa}$ are *non-automorphic*).

---

* (1) Euler, *Comment. Arithm.*, Petropol., 1849, t. II., Paper 59. The proof is *limited* to the case when $\mu_0 \nu_0$ is $+$; *x, x' both odd*, or *both even*; *y, y' both odd* or *both even*.

(2) Legendre, *Théorie des Nombres*, 3rd ed., Paris, 1830, t. I., Art. 236–240. The proof is limited to the case when $\mu_0 \nu_0$ is $+$, (more general than Euler's).

(3) These restrictions have been *removed* in a (verbal) communication by the present author to the London Mathematical Society (*Proc.*, Vol. XXXII., p. 164).

Examples.—In (1), $\mu\nu$ is + ; in (2), $\mu\nu$ is − ; whilst (3) illustrates a *failure* under Rule (10).

(1) *Given* $N = \Phi_2 = \Phi_2' = 40991$; $\Phi_2 = 5 \,.\, 54^2 + 11 \,.\, 49^2$, $\Phi_2' = 5 \,.\, 78^2 + 11 \,.\, 31^2$;

Here $D = \dfrac{78^2 - 54^2}{11} = \dfrac{49^2 - 31^2}{5} = 12 \,.\, 24$; $\mathfrak{N} = (78 \,.\, 49)^2 - (54 \,.\, 31)^2$;

therefore

$$\mathfrak{N} = (3822 - 1674)(3822 + 1674), \quad \text{and} \quad N = \frac{\mathfrak{N}}{D} = \frac{2148 \,.\, 5496}{12 \,.\, 24} = 179 \,.\, 229.$$

(2) *Given* $N = \Phi_2 = \Phi_2' = 817$; $\Phi_2 = 3 \,.\, 17^2 - 2 \,.\, 5^2$, $\Phi_2' = 3 \,.\, 25^2 - 2 \,.\, 23^2$;

Here $D = \dfrac{25^2 - 17^2}{-2} = \dfrac{5^2 - 23^2}{3} = -12 \,.\, 14$; $\mathfrak{N} = (25 \,.\, 5)^2 - (17 \,.\, 23)^2$;

therefore $\mathfrak{N} = (125 - 391)(125 + 391)$, and $N = \dfrac{\mathfrak{N}}{D} = \dfrac{-266 \,.\, 516}{-14 \,.\, 12} = 19 \,.\, 43.$

(3) *Given* $N = \Phi_2 = \Phi_2' = 817$; $\Phi_2 = 3 \,.\, 17^2 - 2 \,.\, 5^2$, $\Phi_2' = 3 \,.\, 65^2 - 2 \,.\, 77^2$;

Here $D = \dfrac{65^2 - 17^2}{-2} = \dfrac{5^2 - 77^2}{3} = -2 \,.\, 984$; $\mathfrak{N} = (65 \,.\, 5)^2 - (17 \,.\, 77)^2$;

therefore $\mathfrak{N} = (325 - 1309)(325 + 1309)$, and $N = \dfrac{\mathfrak{N}}{D} = \dfrac{-984 \,.\, 1634}{-984 \,.\, 2} = 817$;

Here the process *fails* to factorise N, although N is *composite* (= 19 . 43), in consequence of $L = -984$ being a factor of D [see Rule (8*b*)]. This indicates that the data are *unsuitable* under Rule (10) ; in fact Φ_2, Φ_2' are *Automorphs* ; for $\Phi_2 \,.\, \phi_2 = \Phi_2'$ *identically* by the rules of conformal multiplication, taking $\phi_2 = 5^2 - 6 \,.\, 2^2 = 1$ (a *unit-form* conformal with Φ_2). Compare Ex. (2) above, where the factorisation of the same number N *succeeds*, (the forms Φ_2, Φ_2' being *non-equivalent*).

9. *Antimorph Quadratics* (Φ_2, Φ_2').—In Art. 7, take

$$k = 2, \quad j = -1, \tag{20}$$

giving $\Phi_2 = \mu_0 x^2 + \nu_0 y^2$, $\Phi_2' = \mu_0 x'^2 - \nu_0 y'^2$; $[N = \Phi_2 = \Phi_2']$. (21)

Therefore

$$D = \frac{x'^2 - x^2}{\nu_0} = \frac{y^2 + y'^2}{\mu_0} = integer ; \tag{22}$$

therefore

$$\mathfrak{N} = (x'y)^2 + (xy')^2 = (x'y + xy')^2 - 2xyx'y' \tag{23}$$

$$= P^2 - Q^2, \text{ a } \textit{difference of squares}, \text{ when } 2xyx'y' = Q^2. \tag{23a}$$

The condition (23*a*), that $\mathfrak{N}$ shall become a *difference of squares*, may be satisfied in sixteen principal (quite simple) ways, which fall naturally into *four* classes, each of *four* cases, as in following scheme :—

Class...	I	II	III	IV
Case...	1°, 2°, 3°, 4°	5°, 6°, 7°, 8°	9°, 10°, 11°, 12°	13°, 14°, 15°, 16°
$x =$	x , $2y'$, y' , x	ξ^2, $2y'$, ξ^2 , x	$2\xi^2$, ξ^2 , x , y'	$2\xi^2$, ξ^2 , ξ^2, ξ^2
$y =$	y , x' , $2x'$, y	y , η^2 , $2x'$, η^2	y , x' , $2\eta^2$, η^2	η^2, η^2 , $2\eta^2$, η^2
$x' =$	$2y$, x' , x' , y	$2y$, ξ'^2, x' , ξ'^2	y , x' , ξ'^2, $2\xi'^2$	ξ'^2, ξ'^2 , ξ'^2 , $2\xi'^2$
$y' =$	x , y' , y' , $2x$	η'^2, y' , η'^2 , $2x$	η'^2, $2\eta'^2$, x , y'	η'^2, $2\eta'^2$, η'^2 , η'^2

A brief detail of each Case (1°–16°), showing the values of Φ_2, Φ_2', D (in *two* forms), and $\mathfrak{Y}$, is given in the table below.

Class.	Case.	Φ_2	Φ_2'	D	$\mathfrak{Y}$
I,	1°	$\mu_0x^2+\nu_0y^2$,	$4\mu_0y^2-\nu_0x^2$	$(4y^2-x^2)/\nu_0=(y^2+x^2)/\mu_0$	$4y^4+x^4$
	2°	$4\mu_0y'^2+\nu_0x'^2$,	$\mu_0x'^2-\nu_0y'^2$	$(x'^2-4y'^2)/\nu_0=(x'^2+y'^2)/\mu_0$	$x'^4+4y'^4$
	3°	$\mu_0y'^2+4\nu_0x'^2$,	$\mu_0x'^2-\nu_0y'^2$	$(x'^2-y'^2)/\nu_0=(4x'^2+y'^2)/\mu_0$	$4x'^4+y'^4$
	4°	$\mu_0x^2+\nu_0y^2$,	$\mu_0y^2-4\nu_0x^2$	$(y^2-x^2)/\nu_0=(y^2+4x^2)/\mu_0$	y^4+4x^4
II,	5°	$\mu_0\xi^4+\nu_0y^2$,	$4\mu_0y^2-\nu_0\eta'^4$	$(4y^2-\xi^4)/\nu_0=(y^2+\eta'^4)/\mu_0$	$4y^4+(\xi\eta')^4$
	6°	$4\mu_0y'^2+\nu_0\eta^4$,	$\mu_0\xi'^4-\nu_0y'^2$	$(\xi'^4-4y'^2)/\nu_0=(\eta^4+y'^2)/\mu_0$	$(\xi'\eta)^4+4y'^4$
	7°	$\mu_0\xi^4+4\nu_0x'^2$,	$\mu_0x'^2-\nu_0\eta'^4$	$(x'^2-\xi^4)/\nu_0=(4x'^2+\eta'^4)/\mu_0$	$4x'^4+(\xi\eta')^4$
	8°	$\mu_0x^2+\nu_0\eta^4$,	$\mu_0\xi'^4-4\nu_0x^2$	$(\xi'^4-x^2)/\nu_0=(\eta^4+4x^2)/\mu_0$	$(\xi'\eta)^4+4x^4$
III,	9°	$4\mu_0\xi^4+\nu_0y^2$,	$\mu_0y^2-\nu_0\eta'^4$	$(y^2-4\xi^4)/\nu_0=(y^2+\eta'^4)/\mu_0$	$y^4+4(\xi\eta')^4$
	10°	$\mu_0\xi^4+\nu_0x'^2$,	$\mu_0x'^2-4\nu_0\eta'^4$	$(x'^2-\xi^4)/\nu_0=(x'^2+4\eta'^4)/\mu_0$	$x'^4+4(\xi\eta')^4$
	11°	$\mu_0x^2+4\nu_0\eta^4$,	$\mu_0\xi'^4-\nu_0x^2$	$(\xi'^4-x^2)/\nu_0=(4\eta^4+x^2)/\mu_0$	$4(\xi'\eta)^4+x^4$
	12°	$\mu_0y'^2+\nu_0\eta^4$,	$4\mu_0\xi'^4-\nu_0y'^2$	$(4\xi'^4-y'^2)/\nu_0=(\eta^4+y'^2)/\mu_0$	$4(\xi'\eta)^4+y'^4$
IV,	13°	$4\mu_0\xi^4+\nu_0\eta^4$,	$\mu_0\xi'^4-\nu_0\eta'^4$	$(\xi'^4-4\xi^4)/\nu_0=(\eta^4+\eta'^4)/\mu_0$	$(\xi'\eta)^4+4(\xi\eta')^4$
	14°	$\mu_0\xi^4+\nu_0\eta^4$,	$\mu_0\xi'^4-4\nu_0\eta'^4$	$(\xi'^4-\xi^4)/\nu_0=(\eta^4+4\eta'^4)/\mu_0$	$(\xi'\eta)^4+4(\xi\eta')^4$
	15°	$\mu_0\xi^4+4\nu_0\eta^4$,	$\mu_0\xi'^4-\nu_0\eta'^4$	$(\xi'^4-\xi^4)/\nu_0=(4\eta^4+\eta'^4)/\mu_0$	$4(\xi'\eta)^4+(\xi\eta')^4$
	16°	$\mu_0\xi^4+\nu_0\eta^4$,	$4\mu_0\xi'^4-\nu_0\eta'^4$	$(4\xi'^4-\xi^4)/\nu_0=(\eta^4+\eta'^4)/\mu_0$	$4(\xi'\eta)^4+(\xi\eta')^4$

It will be seen that the binomials Φ_2, Φ_2' take particular forms in each class,

I. *Quadratic;* II., III. *Quadratico-quartic;* IV. *Quartic;*

whilst the final $\mathfrak{N}$ takes *the same form* in all. These values of $\mathfrak{N}$ may be all included in the form, styled* *Bin-Aurifeuillian*,

$$N = X^4 + 4Y^4, \tag{24}$$

whose factors are known* to be

$$L = (X \sim Y)^2 + Y^2, \quad M = (X+Y)^2 + Y^2. \tag{25}$$

Examples.—[The numbering (1°, 2°, &c.) is that of the *Case* referred to.]

1°. *Given* $N = \Phi_2 = \Phi_2' = 221$; $\Phi_2 = 5 \,.\, 3^2 + 11 \,.\, 4^2$, $\Phi_2' = 5 \,.\, 8^2 - 11 \,.\, 3^2$;

Here $D = \dfrac{8^2-3^2}{11} = \dfrac{4^2+3^2}{5} = 5$; $\mathfrak{N} = 4 \,.\, 4^4 + 3^4$;

therefore $\mathfrak{N} = (1^2+4^2)(7^2+4^2) = 17 \,.\, 65$; and $N = \dfrac{17 \,.\, 65}{5} = 17 \,.\, 13$.

2°. *Given* $N = \Phi_2 = \Phi_2' = 481$; $\Phi_2 = 10 \,.\, 2^2 + 9 \,.\, 7^2$, $\Phi_2' = 10 \,.\, 7^2 - 9 \,.\, 1^2$;

Here $D = \dfrac{7^2-2^2}{9} = \dfrac{7^2+1^2}{10} = 5$; $\mathfrak{N} = 7^4 + 4 \,.\, 1^4$;

therefore $\mathfrak{N} = (6^2+1^2)(8^2+1^2) = 37 \,.\, 65$; and $N = \dfrac{37 \,.\, 65}{5} = 37 \,.\, 13$.

3°. *Given* $N = \Phi_2 = \Phi_2' = 205$; $\Phi_2 = 13 \,.\, 1^2 + 3 \,.\, 8^2$, $\Phi_2' = 13 \,.\, 4^2 - 3 \,.\, 1^2$;

Here $D = \dfrac{4^2-1^2}{3} = \dfrac{8^2+1^2}{13} = 5$; $\mathfrak{N} = 4 \,.\, 4^4 + 1^4$;

$\mathfrak{N} = (3^2+4^2)(5^2+4^2) = 25 \,.\, 41$; $N = \dfrac{25 \,.\, 41}{5} = 5 \,.\, 41$.

4°. *Given* $N = \Phi_2 = \Phi_2' = 493$; $\Phi_2 = 13 \,.\, 2^2 + 9 \,.\, 7^2$, $\Phi_2' = 13 \,.\, 7^2 - 9 \,.\, 4^2$;

Here $D = \dfrac{7^2-2^2}{9} = \dfrac{7^2+4^2}{13} = 5$; $\mathfrak{N} = 7^4 + 4 \,.\, 2^4$;

therefore $\mathfrak{N} = (5^2+2^2)(9^2+2^2) = 29 \,.\, 85$; $N = \dfrac{29 \,.\, 85}{5} = 29 \,.\, 17$.

5°. *Given* $N = \Phi_2 = \Phi_2' = 1937$; $\Phi_2 = 10 \,.\, 3^4 + 23 \,.\, 7^2$, $\Phi_2' = 4 \,.\, 10 \,.\, 7^2 - 23 \,.\, 1^4$,

Here $D = \dfrac{4 \,.\, 7^2-3^4}{23} = \dfrac{7^2+1^4}{10} = 5$; $\mathfrak{N} = 4 \,.\, 7^4 + 3^4$;

therefore $\mathfrak{N} = (4^2+7^2)(10^2+7^2) = 65 \,.\, 149$; and $N = \dfrac{65 \,.\, 149}{5} = 13 \,.\, 149$.

---

* *Bin-Aurifeuillian;* a name given to the function (X^4+4Y^4) in the author's paper "On Aurifeuillians" in *Proc. Lond. Math. Soc.*, Vol. xxix.; its properties are there studied.

9°. *Given* $N = \Phi_2 = \Phi_2' = 493$; $\Phi_2 = 4 \,.\, 13 \,.\, 1^4 + 9 \,.\, 7^2$, $\Phi_2' = 13 \,.\, 7^2 - 9 \,.\, 2^4$;

Here $D = \frac{7^2 - 4 \,.\, 1^4}{9} = \frac{7^2 + 2^4}{13} = 5$; $\mathfrak{N} = 7^4 + 4 \,.\, 2^4$;

therefore $\mathfrak{N} = (5^2 + 2^2)(9^2 + 2^2) = 29 \,.\, 85$; and $N = \frac{29 \,.\, 85}{5} = 29 \,.\, 17$.

13°. *Given* $N = \Phi_2 = \Phi_2' = 12017$; $\Phi_2 = 4 \,.\, 146 \,.\, 2^4 + 33 \,.\, 3^4$, $\Phi_2' = 146 \,.\, 5^4 - 33 \,.\, 7^4$;

Here $D = \frac{5^4 - 4 \,.\, 2^4}{33} = \frac{3^4 + 7^4}{146} = 17$; $\mathfrak{N} = (5 \,.\, 3)^4 + 4(2 \,.\, 7)^4$;

therefore

$\mathfrak{N} = (1^2 + 14^2)(29^2 + 14^2) = 197 \,.\, 1037$; and $N = \frac{\mathfrak{N}}{D} = \frac{197 \,.\, 1037}{17} = 197 \,.\, 61$.

10. *Antimorph Cubics* (Φ_3, Φ_3').—In Art. 7, take

$$k = 3, \quad j = -1; \tag{26}$$

giving $\Phi_3 = \mu_0 x^3 + \nu_0 y^3$, $\Phi_3' = \mu_0 x'^3 - \nu_0 y'^3$; $[N = \Phi_3 = \Phi_3']$, (27)

therefore $D = \frac{x'^3 - x^3}{\nu_0} = \frac{y^3 + y'^3}{\mu_0} = integer$, (28)

$$\mathfrak{H} = (x'y)^3 + (xy')^3 = F_3 . \mathfrak{F}_3, \text{ suppose}, \tag{29}$$

where $F_3 = x'y + xy'$, $\mathfrak{F}_3 = \{(x'y)^3 + (xy')^3\} \div (x'y + xy')$. (30)

Then $\mathfrak{F}_3 = (x'y + xy')^2 - 3xyx'y'$ (31)

$= P^2 - Q^2$, a *difference of squares*, when $3xyx'y' = Q^2$. (31*a*)

The condition (31*a*) that $\mathfrak{F}_3$ shall become a *difference of squares* may be satisfied in sixteen principal (quite simple) ways, falling naturally into *four* classes of *four* sub-cases each.

Class...	I				II				III				IV			
Case ...	1°,	2°,	3°,	4°	5°,	6°,	7°,	8°	9°,	10°,	11°,	12°	13°,	14°,	15°,	16°
$x =$	x,	$3y'$,	y',	x	ξ^2,	$3y'$,	ξ^2,	x	$3\xi^2$,	ξ^2,	x,	y'	$3\xi^2$,	ξ^2,	ξ^2,	ξ^2
$y =$	y,	x',	$3x'$,	y	y,	η^2,	$3x'$,	η'^2	y,	x',	$3\eta^2$,	η^2	η^2,	η^2,	$3\eta^2$,	η^2
$x' =$	$3y$,	x',	x',	y	$3y$,	ξ'^2,	x',	ξ'^2	y,	x',	ξ'^2,	$3\xi'^2$	ξ'^2,	ξ'^2,	ξ'^2,	$3\xi'^2$
$y' =$	x,	y',	y',	$3x$	η'^2,	y'.	η'^2,	$3x$	η'^2,	$3\eta'^2$,	x,	y'	η'^2,	$3\eta'^2$,	η'^2,	η'^2

A brief detail of each Case (1°–16°), showing the values of Φ_3, Φ_3', D (*two* forms), and $\mathfrak{H}$ is given below. It will be seen that the binomials Φ_3, Φ_3' take particular forms in each class, viz.,

I. *Cubic;* II., III. *Cubo-sextic;* IV. *Sextic,* whilst the final $\mathfrak{N}$ takes *the same form* in all. These values of $\mathfrak{N}$ may be all included in the one formula

$$\mathfrak{N} = X^6+3^3 . Y^6 = F_3 . \mathfrak{F}_3, \text{ suppose,} \tag{32}$$

where $$F_3 = X^2+3Y^2, \quad \mathfrak{F}_3 = (X^6+3^3 . Y^6) \div (X^2+3Y^2), \tag{33}$$

the factor $\mathfrak{F}_3$ being what is styled a *Trin-Aurifeuillian;** whose factors are known* to be

$$L = X^2-3XY+3Y^2 = F_3-3XY, \quad M = X^2+3XY+3Y^2 = F_3+3XY. \tag{34}$$

Class.	Case.	Φ_3	Φ_3'	D	$\mathfrak{N}$
I,	1°	$\mu_0 x^3+\nu_0 y^3$,	$3^3\mu_0 y^3-\nu_0 x^3$	$(3^3y^3-x^3)/\nu_0 = (y^3+x^3)/\mu_0$	$3^3y^6+x^6$
	2°	$3^3\mu_0 y'^3+\nu_0 x'^3$,	$\mu_0 x'^3-\nu_0 y'^3$	$(x'^3-3^3y'^3)/\nu_0 = (x'^3+y'^3)/\mu_0$	$x'^6+3^3y'^6$
	3°	$\mu_0 y'^3+3^3\nu_0 x'^3$,	$\mu_0 x'^3-\nu_0 y'^3$	$(x'^3-y'^3)/\nu_0 = (3^3x'^3+y'^3)/\mu_0$	$3^3x'^6+y'^6$
	4°	$\mu_0 x^3+\nu_0 y^3$,	$\mu_0 y^3-3^3\nu_0 x^3$	$(y^3-x^3)/\nu_0 = (y^3+3^3x^3)/\mu_0$	$y^6+3^3x^6$
II,	5°	$\mu_0\xi^6+\nu_0 y^3$,	$3^3\mu_0 y^3-\nu_0\eta'^6$	$(3^3y^3-\xi^6)/\nu_0 = (y^3+\eta'^6)/\mu_0$	$3^3y^6+(\xi\eta')^6$
	6°	$3^3\mu_0 y'^3+\nu_0\eta^6$,	$\mu_0\xi'^6-\nu_0 y'^3$	$(\xi'^6-3^3y'^3)/\nu_0 = (\eta^6+y'^3)/\mu_0$	$(\xi'\eta)^6+3^3y'^6$
	7°	$\mu_0\xi^6+3^3\nu_0 x'^3$,	$\mu_0 x'^3-\nu_0\eta'^6$	$(x'^3-\xi^6)/\nu_0 = (3^3x'^3+\eta'^6)/\mu_0$	$3^3x'^6+(\xi\eta')^6$
	8°	$\mu_0 x^3+\nu_0\eta'^6$,	$\mu_0\xi'^6-3^3\nu_0 x^3$	$(\xi'^6-x^3)/\nu_0 = (\eta'^6+3^3x^3)/\mu_0$	$(\xi'\eta)^6+3^3x^6$
III,	9°	$3^3\mu_0\xi^6+\nu_0 y^3$,	$\mu_0 y^3-\nu_0\eta'^6$	$(y^3-3^3\xi^6)/\nu_0 = (y^3+\eta'^6)/\mu_0$	$y^6+3^3(\xi\eta')^6$
	10°	$\mu_0\xi^6+\nu_0 x'^3$,	$\mu_0 x'^3-3^3\nu_0\eta'^6$	$(x'^3-\xi^6)/\nu_0 = (x'^3+3^3\eta'^6)/\mu_0$	$x'^6+3^3(\xi\eta')^6$
	11°	$\mu_0 x^3+3^3\nu_0\eta^6$,	$\mu_0\xi'^6-\nu_0 x^3$	$(\xi'^6-x^3)/\nu_0 = (3^3\eta^6+x^3)/\mu_0$	$3^3(\xi'\eta)^6+x^6$
	12°	$\mu_0 y'^3+\nu_0\eta^6$,	$3^3\mu_0\xi'^6-\nu_0 y'^3$	$(3^3\xi'^6-y'^3)/\nu_0 = (\eta^6+y'^3)/\mu_0$	$3^3(\xi'\eta)^6+y'^6$
IV,	13°	$3^3\mu_0\xi^6+\nu_0\eta^6$,	$\mu_0\xi'^6-\nu_0\eta'^6$	$(\xi'^6-3^3\xi^6)/\nu_0 = (\eta^6+\eta'^6)/\mu_0$	$(\xi'\eta)^6+3^3(\xi\eta')^6$
	14°	$\mu_0\xi^6+\nu_0\eta^6$,	$\mu_0\xi'^6-3^3\nu_0\eta'^6$	$(\xi'^6-\xi^6)/\nu_0 = (\eta^6+3^3\eta'^6)/\mu_0$	$(\xi'\eta)^6+3^3(\xi\eta')^6$
	15°	$\mu_0\xi^6+3^3\nu_0\eta^6$,	$\mu_0\xi'^6-\nu_0\eta'^6$	$(\xi'^6-\xi^6)/\nu_0 = (3^3\eta^6+\eta'^6)/\mu_0$	$3^3(\xi'\eta)^6+(\xi\eta')^6$
	16°	$\mu_0\xi^6+\nu_0\eta^6$,	$3^3\mu_0\xi'^6-\nu_0\eta'^6$	$(3^3\xi'^6-\xi^6)/\nu_0 = (\eta^6+\eta'^6)/\mu_0$	$3^3(\xi'\eta)^6+(\xi\eta')^6$

It will be seen that $\mathfrak{N}$ has been resolved into *three* factors, $\mathfrak{N} = F_3 . L . M$, and that N itself is therefore also usually hereby resolvable into *three* factors (Art. **4a**).

---

* *Trin-Aurifeuillian*; a name given to the function $(X^6+3^3Y^6) \div (X^2+3Y^2)$ in the author's paper "On Aurifeuillians" above quoted; its properties are there studied.

Examples.—[The numbering (1°, 2°, &c.) is that of the *Case* referred to.]

1°. *Given* $N = \Phi_3 = \Phi'_3 = 2821$; $\Phi_3 = 5 . 2^3 + 103 . 3^3$, $\Phi'_3 = 3^3 . 5 . 3^3 - 103 . 2^3$;

Here $D = \frac{(3 . 3)^3 - 2^3}{103} = \frac{3^3 + 2^3}{5} = 7$; $\mathfrak{N} = 3^3 . 3^6 + 2^6$; $F_3 = 3 . 3^2 + 2^2 = 31$;

therefore

$\mathfrak{N} = 31\,(31 - 3 . 2 . 3)(31 + 3 . 2 . 3)$; and $N = \frac{\mathfrak{N}}{D} = \frac{31 . 13 . 49}{7} = 31 . 13 . 7.$

2°. *Given* $N = \Phi_3 = \Phi'_3 = 142861$;

$\Phi_3 = 3^3 . 143 . 1^3 + 139 . 10^3$, $\Phi'_3 = 143 . 10^3 - 139 . 1^3$;

Here $D = \frac{10^3 - 3^3 . 1^3}{139} = \frac{10^3 + 1^3}{143} = 7$; $\mathfrak{N} = 10^6 + 3^3 . 1^6$; $F_3 = 10^2 + 3 . 1^2 = 103$;

therefore

$\mathfrak{N} = 103\,(103 - 3 . 10)(103 + 3 . 10)$; and $N = \frac{\mathfrak{N}}{D} = \frac{103 . 73 . 133}{7} = 103 . 73 . 19.$

5°. *Given* $N = \Phi_5 = \Phi'_3 = 60277$;

$\Phi_3 = 27 . 1^6 + 482 . 5^3$, $\Phi'_3 = 3^3 . 27 . 5^3 - 482 . 2^6$;

Here $D = \frac{3^3 . 5^3 - 1^6}{482} = \frac{5^3 + 2^6}{27} = 7$; $\mathfrak{N} = 3^3 . 5^6 + (1 . 2)^6$; $F_3 = 3 . 5^2 + 2^2 = 79$:

therefore

$\mathfrak{N} = 79\,(79 - 3 . 5 . 2)(79 + 3 . 5 . 2)$; and $N = \frac{\mathfrak{N}}{D} = \frac{79 . 49 . 109}{7} = 79 . 7 . 109.$

9°. *Given* $N = \Phi_3 = \Phi'_3 = 689791$;

$\Phi_3 = 3^3 . 323 . 1^6 + 310 . 13^3$, $\Phi'_3 = 323 . 13^3 - 310 . 2^6$;

Here $D = \frac{13^3 - 3^3 . 1^6}{310} = \frac{13^3 + 2^6}{323} = 7$; $\mathfrak{N} = 13^6 + 3^3\,(1 . 2)^6$; $F_3 = 13^2 + 3 . 2^2 = 181$;

therefore $\mathfrak{N} = 181\,(181 - 3 . 13 . 2)(181 + 3 . 13 . 2)$;

and $N = \frac{\mathfrak{N}}{D} = \frac{181 . 103 . 259}{7} = 181 . 103 . 37.$

13°. *Given* $N = \Phi_3 = \Phi'_3 = 21679$;

$\Phi_3 = 3^3 . 61 . 1^6 + 313 . 2^6$, $\Phi'_3 = 61 . 4^6 - 313 . 3^6$;

Here $D = \frac{4^6 - 3^3 . 1^6}{313} = \frac{2^6 + 3^6}{61} = 13$; $\mathfrak{N} = (4 . 2)^6 + 3^3\,(1 . 3)^6$, $F_3 = 8^2 + 3 . 3^2 = 91$;

therefore

$\mathfrak{N} = 91\,(91 - 3 . 8 . 3)(91 + 3 . 8 . 3)$, and $N = \frac{\mathfrak{N}}{D} = \frac{91 . 19 . 163}{13} = 7 . 19 . 163.$

11. *Quasi-Conformals, and Anti-Quasi-Conformals* (Φ_k, Φ'_k).—These are the next most simple *general* forms (Φ_k, Φ'_k) leading to the simplest factorisable form (11) of $\mathfrak{H}$. They are defined by writing in Art. **3**,

$$\mu = n^{\alpha}.\mu_0,\quad \nu = m^{\beta}.\nu_0,\quad \mu' = m^{\gamma}.\mu_0,\quad \nu' = j.n^{\delta}.\nu_0;\ \text{where } j = \pm 1, \tag{35}$$

with the conditions
$$\beta+\gamma = \alpha+\delta = k, \tag{36}$$

giving
$$\frac{\mu\nu'}{\mu'\nu} = j\,\frac{n^{\alpha+\delta}}{n^{\beta+\gamma}} = j\left(\frac{n}{m}\right)^k. \tag{36a}$$

Then
$$\Phi_k = n^{\alpha}\mu_0.x^k + m^{\beta}\nu_0.y^k,\quad \Phi'_k = m^{\gamma}\mu_0.x'^k + j.n^{\delta}\nu_0.y'_k, \tag{37}$$

$$D = \frac{m^{\gamma}x'^k - n^{\alpha}x^k}{\nu_0} = \frac{m^{\beta}y^k - j.n^{\delta}y'^k}{\mu_0} = \textit{integer}, \tag{38}$$

$$\begin{aligned}\mathfrak{H} &= m^{\beta+\gamma}(x'y)^k - j.n^{\alpha+\delta}(xy')^k \\ &= (mx'y)^k - j(nxy')^k,\end{aligned} \tag{39}$$

which is of the *general* form (11) required.

The forms Φ_k, Φ'_k of (37) are seen—by (36a)—to be *Quasi-conformals* when $j = +1$, and *Anti-quasi-conformals* when $j = -1$ (Art. **6**). These forms (37) include both *Conformals* and *Anti-conformals* (Art. **6**), when $k = 2\kappa$; for, writing

$$k = 2\kappa,\ \alpha = \beta = \gamma = \delta = \kappa \ \text{ in (35)}$$

gives
$$\mu\nu = \pm\mu'\nu'. \tag{40}$$

It is proposed to consider only the simpler, and more interesting, cases, given by $k = 2$, $j = \pm 1$, and by $k = 3$, $j = -1$ (Arts. **12**, **13**, **13a**, **14**, **14a**).

12. *Conformal Quadratics* (Φ_2, Φ'_2).—In Art. **11**, take

$$k = 2\kappa,\quad \alpha = \beta = \gamma = \delta = \kappa,\quad j = +1, \tag{41}$$

giving
$$\mu = n^{\kappa}\mu_0,\quad \nu = m^{\kappa}\nu_0,\quad \mu' = m^{\kappa}\mu_0,\quad \nu' = n^{\kappa}\nu_0; \tag{42}$$

whence $\mu\nu = (mn)^{\kappa}\mu_0\nu_0 = \mu'\nu'$, the condition of *conformality*. (42a)

Then
$$\Phi_{2\kappa} = n^{\kappa}\mu_0.x^{2\kappa} + m^{\kappa}\nu_0.y^{2\kappa},\quad \Phi'_{2\kappa} = m^{\kappa}\mu_0.x'^{2\kappa} + n^{\kappa}\nu_0.y'^{2\kappa}, \tag{43}$$

$$D = \frac{m^{\kappa}x'^{2\kappa} - n^{\kappa}x^{2\kappa}}{\nu_0} = \frac{m^{\kappa}y^{2\kappa} - n^{\kappa}y'^{2\kappa}}{\mu_0} = \textit{integer}, \tag{44}$$

$$\mathfrak{H} = (mx'y)^{2\kappa} - (nxy')^{2\kappa},\ \text{a } \textit{difference of squares}. \tag{45}$$

Here the twin forms ($\Phi_{2\kappa}$, $\Phi'_{2\kappa}$) are *conformal quadratic forms*, a case believed* to be always factorisable (when $\Phi_{2\kappa}$, $\Phi'_{2\kappa}$ are *non-automorphic*).

Examples.—In (1), $\mu\nu$ is $+$: in (2), $\mu\nu$ is $-$; whilst (3) illustrates a *failure* under Rule (10).

(1) *Given* $N = \Phi_2 = \Phi'_2 = 6989$;

$$\Phi_2 = 3 . 43 . 1^2 + 5 . 7 . 14^2, \quad \Phi'_2 = 5 . 43 . 4^2 + 3 . 7 . 13^2;$$

Here $D = \frac{5 . 4^2 - 3 . 1^2}{7} = \frac{5 . 14^2 - 3 . 13^2}{43} = 11$; $\mathfrak{N} = (5 . 4 . 14)^2 - (3 . 1 . 13)^2$;

therefore $\mathfrak{N} = (280-39)(280+39)$; and $\mathfrak{N} = \frac{\mathfrak{N}}{D} = \frac{241 . 319}{11} = 241 . 29.$

(2) *Given* $N = \Phi_2 = \Phi'_2 = 2501$;

$$\Phi_2 = 3 . 7 . 11^2 - 5 . 2 . 2^2, \quad \Phi'_2 = 5 . 7 . 11^2 - 3 . 2 . 17^2;$$

Here $D = \frac{5 . 11^2 - 3 . 11^2}{-2} = \frac{5 . 2^2 - 3 . 17^2}{7} = -121$; $\mathfrak{N} = (5 . 11 . 2)^2 - (3 . 11 . 17)^2$;

therefore $\mathfrak{N} = (110-561)(110+561)$; and $N = \frac{\mathfrak{N}}{D} = \frac{-451 . 671}{-11 . 11} = 41 . 61.$

(3) *Given* $N = \Phi_2 = \Phi'_2 = 2501$;

$$\Phi_2 = 3 . 7 . 11^2 - 5 . 2 . 2^2, \quad \Phi'_2 = 5 . 7 . 29^2 - 3 . 2 . 67^2;$$

Here $D = \frac{5 . 29^2 - 3 . 11^2}{-2} = \frac{5 . 2^2 - 3 . 67^2}{7} = -1921$; $\mathfrak{N} = (5 . 29 . 2)^2 - (3 . 11 . 67)^2$;

therefore $\mathfrak{N} = (290-2211)(290+2211)$; and $N = \frac{\mathfrak{N}}{D} = \frac{-1921 . 2501}{-1921} = 2501.$

Here the process *fails* to factorise N, although N is composite ($= 41 . 61$), in consequence of $L = -1921$ being $= D$ [see Rule (8*b*)]. This indicates that the data are *unsuitable* under Rule (10); in fact, Φ_2, Φ'_2 are *Automorphs*; for $\Phi_2 . \phi_2 = \Phi'_2$ *identically* by the rules of conformal multiplication, taking $\phi_2 = 15 . 1^2 - 14 . 1^2 = 1$ (a *unit-form* conformal with Φ_2). Compare Ex. (2) above, where the factorisation of the same number N *succeeds* (the forms Φ_2, Φ'_2 being *non-equivalent*).

13. *Anti-conformal Quadratics* (Φ_2, Φ'_2).—In Art. **11**, take

$$k = 2, \quad \alpha = \beta = \gamma = \delta = \tfrac{1}{2}k = 1, \quad j = -1, \tag{46}$$

giving $$\mu = n\mu_0, \quad \nu = m\nu_0, \quad \mu' = m\mu_0, \quad \nu' = -n\mu_0; \tag{47}$$

whence $\mu\nu = -\mu'\nu'$, the condition of *anticonformality* (Art. **6**), **(47*a*)**

$$\Phi_2 = n\mu_0 . x^2 + m\nu_0 . y^2, \quad \Phi'_2 = m\mu_0 . x'^2 - n\nu_0 . y'^2, \tag{48}$$

---

* Announced in a verbal communication by the author to the London Mathematical Society (*Proceedings*, Vol. xxxii., p. 164).

$$D = \frac{mx'^2 - nx^2}{\nu_0} = \frac{my^2 + ny'^2}{\mu_0} = \text{integer}, \tag{49}$$

$$\mathfrak{N} = (mx'y)^2 + (nxy')^2 = (mx'y + nxy')^2 - 2mnxyx'y' \tag{50}$$

$$= P^2 - Q^2, \text{ a } \textit{difference of squares}, \text{ when } 2mnxyx'y' = Q^2. \tag{50a}$$

The condition (50*a*), that $\mathfrak{N}$ shall become a *difference of squares*, may be satisfied in at least forty-eight principal (quite simple) ways falling naturally into *nine* classes. On account of the great number of cases, an abstract only is given showing the values of m, n, x, y, x', y' defining the cases.

Class...	I–IV	V	VI	VII*	VIII*	IX
Case ...	1°–16°	17°, 18°	19°, 20°, 21°, 22°	23°–28°, 29°–34°	35°–40°, 41°–46°	47°, 48°
$m =$	m_0^2	$2m_0^2$, m_0^2	$2m_0^2$, $2m_0^2$, m_0^2, m_0^2	x', y	x', y	$2m_0^2$, m_0^2
$n =$	n_0^2	n_0^2, $2n_0^2$	n_0^2, n_0^2, $2n_0^2$, $2n_0^2$	y', x	x, y'	n_0^2, $2n_0^2$
$x =$	16 Cases as in Art. 9	x, x	ξ^2, y', ξ^2, y'	ξ^2, x	x, ξ^2	ξ^2, ξ^2
$y =$		y, y	y, η^2, y, η^2	η^2, y	η^2, y	η^2, η^2
$x' =$		y, y	y, ξ'^2, y, ξ'^2	x', ξ'^2	x', ξ'^2	ξ'^2, ξ'^2
$y' =$		x, x	η'^2, y', η'^2, y'	y', η'^2	η'^2, y'	η'^2, η'^2

* Prefix 2 to any one of m, n, x, y, x', y'; each column yields six cases.

In consequence of the complexity of the results no attempt will be made to give any detail of the above in their *general* form. Suffice to say that the binomials Φ_2, Φ_2' take particular forms in each class, viz.,

I–IV. As in Art. **9**; V. *Quadratic*; VI. *Quadratico-quartic*;
VII, VIII. *Cubic and Quintic*; IX. *Biquadratic*,

and that $\mathfrak{N}$ becomes a *Bin-Aurifeuillian*,* and therefore always resolvable, by (24), (25).

13a. *Simpler Anti-conformal Quadratics* (Φ_2, Φ_2').—By taking

$$m_0 = 1, \quad n_0 = 1, \tag{51}$$

in Art **13**, all the forms of Classes I–IV, V, VI, IX are much simplified. Thus Classes I–IV become identical with those of same number in Art. **9**, so need not be further considered.

---

* See foot-note * of Art. **9**, p. 367.

Classes V, VI, IX.—Taking $m_0 = 1$, $n_0 = 1$ gives $(m, n) = (2, 1)$ or $(1, 2)$. A brief detail of each case (17°, 18°; 19°–22°; 47°, 48°) of these three classes, showing the values of Φ_2, Φ_2', D (two forms), and $\mathfrak{N}$, is given below. It will be seen that the binomials Φ_2, Φ_2' take the particular forms stated (Art. 13), and that $\mathfrak{N}$ takes the *same form* in all, viz., the *Bin-Aurifeuillian* $(X^4 + 4Y^4)$, whose factorisation is given in (24), (25).

Class.	Case.	m, n	Φ_2	Φ_2'	D	$\mathfrak{N}$
V,	17°	2, 1	$\mu_0 x^2 + 2\nu_0 y^2$,	$2\mu_0 y^2 - \nu_0 x^2$	$(2y^2 - x^2)/\nu_0 = (2y^2 + x^2)/\mu_0$	$4y^4 + x^4$
	18°	1, 2	$2\mu_0 x^2 + \nu_0 y^2$,	$\mu_0 y^2 - 2\nu_0 x^2$	$(y^2 - 2x^2)/\nu_0 = (y^2 + 2x^2)/\mu_0$	$y^4 + 4x^4$
VI,	19°	2, 1	$\mu_0 \xi^4 + 2\nu_0 y^2$,	$2\mu_0 y^2 - \nu_0 \eta'^4$	$(2y^2 - \xi^4)/\nu_0 = (2y^2 + \eta'^4)/\mu_0$	$4y^4 + (\xi\eta')^4$
	20°	2, 1	$\mu_0 y'^2 + 2\nu_0 \eta^4$,	$2\mu_0 \xi'^4 - \nu_0 y'^2$	$(2\xi'^4 - y'^2)/\nu_0 = (2\eta^4 + y'^2)/\mu_0$	$4(\xi'\eta)^4 + y'^4$
	21°	1, 2	$2\mu_0 \xi^4 + \nu_0 y^2$,	$\mu_0 y^2 - 2\nu_0 \eta'^4$	$(y^2 - 2\xi^4)/\nu_0 = (y^2 + 2\eta'^4)/\mu_0$	$y^4 + 4(\xi\eta')^4$
	22°	1, 2	$2\mu_0 y'^2 + \nu_0 \eta^4$,	$\mu_0 \xi'^4 - 2\nu_0 y'^2$	$(\xi'^4 - 2y'^2)/\nu_0 = (\eta^4 + 2y'^2)/\mu_0$	$(\xi'\eta)^4 + 4y'^4$
IX,	47°	2, 1	$\mu_0 \xi^4 + 2\nu_0 \eta^4$,	$2\mu_0 \xi'^4 - \nu_0 \eta'^4$	$(2\xi'^4 - \xi^4)/\nu_0 = (2\eta^4 + \eta'^4)/\mu_0$	$4(\xi'\eta)^4 + (\xi\eta')^4$
	48°	1, 2	$2\mu_0 \xi^4 + \nu_0 \eta^4$,	$\mu_0 \xi'^4 - 2\nu_0 \eta'^4$	$(\xi'^4 - 2\xi^4)/\nu_0 = (\eta^4 + 2\eta'^4)/\mu_0$	$(\xi'\eta)^4 + 4(\xi\eta')^4$

It will be seen also that these Classes V, VI, IX closely resemble Classes I, II and III, IV respectively of Art. **9**, the coefficient 4 which occurs in either Φ_2 or Φ_2' in the latter being split up into its factors 2 . 2, one appearing in each of Φ_2, Φ_2' in the present article.

Examples.—[The numbering (17°, &c.) is that of the *Case* referred to.]

17°. *Given* $N = \Phi_2 = \Phi_2' = 2581$;

$$\Phi_2 = 59 . 3^2 + 2 . 41 . 5^2, \quad \Phi_2' = 2 . 59 . 5^2 - 41 . 3^2;$$

Here $D = \dfrac{2 . 5^2 - 3^2}{41} = \dfrac{2 . 5^2 + 3^2}{59} = 1$; $\mathfrak{N} = 4 . 5^4 + 3^4$;

therefore $\mathfrak{N} = (2^2 + 5^2)(8^2 + 5^2) = 29 . 89$; and $N = \mathfrak{N}$.

18°. *Given* $N = \Phi_2 = \Phi_2' = 689$;

$$\Phi_2 = 2 . 33 . 2^2 + 17 . 5^2, \quad \Phi_2' = 33 . 5^2 - 2 . 17 . 2^2;$$

Here $D = \dfrac{5^2 - 2 . 2^2}{17} = \dfrac{5^2 + 2 . 2^2}{33} = 1$; $\mathfrak{N} = 5^4 + 4 . 2^4$;

therefore $\mathfrak{N} = (3^2 + 2^2)(7^2 + 2^2) = 13 . 53$; and $N = \mathfrak{N}$.

19°. *Given* $N = \Phi_2 = \Phi_2' = 9685;$

$$\Phi_2 = 99\,.\,3^4 + 2\,.\,17\,.\,7^2, \quad \Phi_2' = 2\,.\,99\,.\,7^2 - 17\,.\,1^4;$$

Here $D = \frac{2\,.\,7^2 - 3^4}{17} = \frac{2\,.\,7 + 1^4}{99} = 1; \quad \mathfrak{N} = 4\,.\,7^4 + (3\,.\,1)^4;$

therefore $\mathfrak{N} = (4^2+7^2)(10^2+7^2) = (65\,.\,149); \quad$ and $\quad N = \mathfrak{N}.$

47°. *Given* $N = \Phi_2 = \Phi_2' = 26245;$

$$\Phi_2 = 163\,.\,1^4 + 2\,.\,161\,.\,3^4; \quad \Phi_2' = 2\,.\,163\,.\,3^4 - 161\,.\,1^4;$$

Here $D = \frac{2\,.\,3^4 - 1^4}{161} = \frac{2\,.\,3\ + 1^4}{163} = 1; \quad \mathfrak{N} = 4\,(3\,.\,3)^4 + (1\,.\,1)^4;$

therefore $\mathfrak{N} = (8^2+9^2)(10^2+9^2) = 145\,.\,181; \quad$ and $\quad N = \mathfrak{N}.$

48°. *Given* $N = \Phi_2 = \Phi_2' = 46561;$

$$\Phi_2 = 2\,.\,1331\,.\,2^4 + 49\,.\,3^4, \quad \Phi_2' = 1331\,.\,3^4 - 2\,.\,49\,.\,5^4;$$

Here $D = \frac{3\ - 2\,.\,2^4}{49} = \frac{3^4 + 2\,.\,5^4}{1331} = 1; \quad \mathfrak{N} = (3\,.\,3)^4 + 4\,(2\,.\,5)^4;$

therefore $\mathfrak{N} = (1^2+10^2)(19^2+10^2) = 101\,.\,461; \quad$ and $\quad N = \mathfrak{N}.$

14. *Anti-quasi-conformal Cubics* (Φ_3, Φ_3').—In Art. **11**, take

$$\beta + \gamma = a + \delta = k = 3, \quad j = -1, \tag{52}$$

which satisfy the condition of *anti-quasi-conformality* [see (36*a*)].
Then $(\beta, \gamma) = (2, 1)$ or $(1, 2)$; and $(a, \delta) = (2, 1)$ or $(1, 2)$, (53)

whilst Φ_3, Φ_3', D are as in (37), (38), (54)

and $\mathfrak{N} = (mx'y)^3 + (nxy')^3 = F_3\,.\,\mathfrak{F}_3$, *suppose*, (55)

where $F_3 = mx'y + nxy', \quad \mathfrak{F}_3 = \{(mx'y)^3 + (nxy')^3\} \div (mx'y + nxy').$ (56)

Here $\mathfrak{F}_3 = (mx'y + nxy')^2 - 3mn\,xyx'y'$

$= P^2 - Q^2$, a *difference of squares*, when $3mn\,xyx'y' = Q^2$. (56*a*)

The condition (56*a*) that $\mathfrak{F}_3$ shall become a *difference of squares* may be satisfied in a great number of principal (quite simple) ways. quite similar to those of Art. **13**; these may be arranged into *nine* classes, as in Art. **13**, but with many more cases in each class (about twice as many), on account of the variation in a, β, γ, δ in (53). The binomials Φ_3, Φ_3' take particular forms in each class, mostly *cubic*, *cubico-sextic*, and *sextic;* and the final values of $\mathfrak{N}$ are all of one form $\mathfrak{N} = (X^6 + 3^3\,.\,Y^6)$, of which the factorisation has been given in (32), (33), (34); it is not thought worth while pursuing these further in their *general* forms.

The Classes I–IX are defined by the values of m, n as below :—

Class...	I–IV	V	VI	VII*	VIII*	IX
$m =$	m_0^2	$3m_0^2,\ m_0^2$	$3m_0^2,\ m_0^2$	$x',\ y$	$x',\ y$	$3m_0^2,\ n_0^2$
$n =$	n_0^2	$m_0^2,\ 3n_0^2$	$n_0^2,\ 3n_0^2$	$y',\ x$	$x,\ y'$	$m_0^2,\ 3n_0^2$
				* Prefix 3 to any one of m, n, x, y, x', y'.		

It will be seen that here the coefficient 3 replaces the coefficient 2 of Art. **13**, (compare the table on p. 373).

14a. *Simpler Anti-quasi-conformal Cubics* (Φ_3, Φ_3').—By taking

$$m_0 = 1, \quad n_0 = 1, \tag{57}$$

in Art. **14**, all the forms of Classes I–IV, V, VI, IX are much simplified. Thus Classes I–IV become identical with those of same number in Art. **10**; so need not be further considered.

Classes V, VI, IX.—Taking $m_0 = 1$, $n_0 = 1$ in last article gives $(m, n) = (3, 1)$ or $(1, 3)$. The following scheme shows the values of m^β, m^γ, n^α, n^δ; x, y, x', y' defining the several cases of these three classes. To every case of Art. **13** here correspond* *two* cases :—

Class...	V		VI				IX	
Case...	17°, 17′;	18, 18′	19°, 19′;	20°, 20′;	21°, 21′;	22°, 22′	47°, 47′;	48°, 48′
$m^\beta =$	3^2, 3;	1, 1	3^2, 3;	3^2, 3;	1, 1;	1, 1	3^2, 3;	1, 1
$m^\gamma =$	3, 3^2;	1, 1	3, 3^2;	3, 3^2;	1, 1;	1, 1	3, 3^2;	1, 1
$n^\alpha =$	1, 1;	3^2, 3	1, 1;	1, 1;	3^2, 3;	3^2, 3	1, 1;	3^2, 3
$n^\delta =$	1, 1;	3, 3^2	1, 1;	1, 1;	3, 3^2;	3, 3^2	1, 1;	3, 3^2
$x =$	x		$\xi^2,\ \xi^2$;	$y',\ y'$;	$\xi^2,\ \xi^2$;	$y',\ y'$	ξ^2	
$y =$	y		$y,\ y$;	$\eta^2,\ \eta^2$;	$y,\ y$;	$\eta^2,\ \eta^2$	η^2	
$x' =$	y		$y,\ y$;	$\xi'^2,\ \xi'^2$;	$y,\ y$;	$\xi'^2,\ \xi'^2$	ξ'^2	
$y' =$	x		$\eta'^2,\ \eta'^2$;	$y',\ y'$;	$\eta'^2,\ \eta'^2$;	$y',\ y'$	η'^2	

A brief detail of each case of these three classes, showing the values of Φ_2, Φ_2', D (two forms), and $\mathfrak{H}$, is given below. It will be

---

[*] To facilitate comparison, the same numbering (with distinguishing accents) has been given to the *corresponding* cases of the two articles. Thus Cases 17°, 17′ here correspond to Case 17° of Art. **13.**

seen that the binomials Φ_2, Φ_2' take particular forms in each class, viz.,

V. *Cubic;* VI. *Cubo-Sextic;* IV. *Sextic,*

whilst the final $\mathfrak{N}$ takes *the same form* in all, viz.,

$$\mathfrak{N} = X^6 + 3^3 . Y^6 = F_3 . \mathfrak{F}_3, \tag{58}$$

whose factorisation has been given in (32), (33), (34).

Class.	Case.	Φ_3	Φ_3'	D	$\mathfrak{N}$
V,	17°	$\mu_0 x^3 + 9\nu_0 y^3$,	$3\mu_0 y^3 - \nu_0 x^3$	$(3y^3 - x^3)/\nu_0 = (9y^3 + x^3)/\mu_0$	$3^3 y^6 + x^6$
	17′	$\mu_0 x^3 + 3\nu_0 y^3$,	$9\mu_0 y^3 - \nu_0 x^3$	$(9y^3 - x^3)/\nu_0 = (3y^3 + x^3)/\mu_0$	$3^3 y^6 + x^6$
	18°	$9\mu_0 x^3 + \nu_0 y^3$,	$\mu_0 y^3 - 3\nu_0 x^3$	$(y^3 - 9x^3)/\nu_0 = (y^3 + 3x^3)/\mu_0$	$y^6 + 3^3 x^6$
	18′	$3\mu_0 x^3 + \nu_0 y^3$,	$\mu_0 y^3 - 9\nu_0 x^3$	$(y^3 - 3x^3)/\nu_0 = (y^3 + 9x^3)/\mu_0$	$y^6 + 3^3 x^6$
VI,	19°	$\mu_0 \xi^6 + 9\nu_0 y^3$,	$3\mu_0 y^3 - \nu_0 \eta'^6$	$(3y^3 - \xi^6)/\nu_0 = (9y^3 + \eta'^6)/\mu_0$	$3^3 y^6 + (\xi\eta')^6$
	19′	$\mu_0 \xi^6 + 3\nu_0 y^3$,	$9\mu_0 y^3 - \nu_0 \eta'^6$	$(9y^3 - \xi^6)/\nu_0 = (3y^3 + \eta'^6)/\mu_0$	$3^3 y^6 + (\xi\eta')^6$
	20°	$\mu_0 y'^3 + 9\nu_0 \eta^6$,	$3\mu_0 \xi'^6 - \nu_0 y'^3$	$(3\xi'^6 - y'^3)/\nu_0 = (9\eta^6 + y'^3)/\mu_0$	$3^3 (\xi'\eta)^6 + y'^6$
	20′	$\mu_0 y'^3 + 3\nu_0 \eta^6$,	$9\mu_0 \xi'^6 - \nu_0 y'^3$	$(9\xi'^6 - y'^3)/\nu_0 = (3\eta^6 + y'^3)/\mu_0$	$3^3 (\xi'\eta)^6 + y'^6$
	21°	$9\mu_0 \xi^6 + \nu_0 y^3$,	$\mu_0 y^3 - 3\nu_0 \eta'^6$	$(y^3 - 9\xi^6)/\nu_0 = (y^3 + 3\eta'^6)/\mu_0$	$y^6 + 3^3 (\xi\eta')^6$
	21′	$3\mu_0 \xi^6 + \nu_0 y^3$,	$\mu_0 y^3 - 9\nu_0 \eta'^6$	$(y^3 - 3\xi^6)/\nu_0 = (y^3 + 9\eta'^6)/\mu_0$	$y^6 + 3^3 (\xi\eta')^6$
	22°	$9\mu_0 y'^3 + \nu_0 \eta^6$,	$\mu_0 \xi'^6 - 3\nu_0 y'^3$	$(\xi'^6 - 9y'^3)/\nu_0 = (\eta^6 + 3y'^3)/\mu_0$	$(\xi'\eta)^6 + 3^3 y'^6$
	22′	$3\mu_0 y'^3 + \nu_0 \eta^6$,	$\mu_0 \xi'^6 - 9\nu_0 y'^3$	$(\xi'^6 - 3y'^3)/\nu_0 = (\eta^6 + 9y'^3)/\mu_0$	$(\xi'\eta)^6 + 3^3 y'^6$
IX,	47°	$\mu_0 \xi^6 + 9\nu_0 \eta^6$,	$3\mu_0 \xi'^6 - \nu_0 \eta'^6$	$(3\xi'^6 - \xi^6)/\nu_0 = (9\eta^6 + \eta'^6)/\mu_0$	$3^3 (\xi'\eta)^6 + (\xi\eta')^6$
	47′	$\mu_0 \xi^6 + 3\nu_0 \eta^6$,	$9\mu_0 \xi'^6 - \nu_0 \eta'^6$	$(9\xi'^6 - \xi^6)/\nu_0 = (3\eta^6 + \eta'^6)/\mu_0$	$3^3 (\xi'\eta)^6 + (\xi\eta')^6$
	48°	$9\mu_0 \xi^6 + \nu_0 \eta^6$,	$\mu_0 \xi'^6 - 3\nu_0 \eta'^6$	$(\xi'^6 - 9\xi^6)/\nu_0 = (\eta^6 + 3\eta'^6)/\mu_0$	$(\xi'\eta)^6 + 3^3 (\xi\eta')^6$
	48′	$3\mu_0 \xi^6 + \nu_0 \eta^6$,	$\mu_0 \xi'^6 - 9\nu_0 \eta'^6$	$(\xi'^6 - 3\xi^6)/\nu_0 = (\eta^6 + 9\eta'^6)/\mu_0$	$(\xi'\eta)^6 + 3^3 (\xi\eta')^6$

Examples.—[The numbering (17°, &c.) is that of the *Case* referred to.]

17°. *Given* $N = \Phi_3 = \Phi_3' = 19747$;

$$\Phi_3 = 251 . 2^3 + 9 . 73 . 3^3, \quad \Phi_3' = 3 . 251 . 3^3 - 73 . 2^3;$$

Here $D = \dfrac{3 . 3^3 - 2^3}{73} = \dfrac{9 . 3^3 + 2^3}{251} = 1$; $\mathfrak{N} = 3^3 . 3^6 + 2^6$, $F_3 = 3 . 3^2 + 2^2 = 31$;

therefore $\mathfrak{N} = 31\,(31 - 3 . 3 . 2)(31 + 3 . 3 . 2) = 31 . 13 . 49$; and $N = \mathfrak{N}$.

19°. *Given* $N = \Phi_3 = \Phi_3' = 281827$;

$$\Phi_3 = 4339 . 2^6 + 9 . 17 . 3^3, \quad \Phi_3' = 3 . 4339 . 3^3 - 17 . 4^6;$$

Here $D = \dfrac{3 . 3^3 - 2^6}{17} = \dfrac{9 . 3^3 + 4^6}{4339} = 1$; $\mathfrak{N} = 3^3 . 3^6 + (2 . 4)^6$, $F_3 = 3 . 3^2 + 8^2 = 91$;

therefore $\mathfrak{N} = 91\,(91 - 3 . 8 . 3)(91 + 3 . 8 . 3) = 91 . 19 . 163$; and $N = \mathfrak{N}$.

47°. *Given* $N = \Phi_3 = \Phi'_3 = 281827$;

$$\Phi_3 = 4105 \,.\, 2^6 + 9 \,.\, 2123 \,.\, 1^6, \quad \Phi'_3 = 3 \,.\, 4105 \,.\, 3^6 - 2123 \,.\, 4^6;$$

Here $D = \dfrac{3 \,.\, 3^6 - 2^6}{2123} = \dfrac{9 \,.\, 1^6 + 4^6}{4105} = 1$; $\mathfrak{N} = 3^3 (3 \,.\, 1)^6 + (2 \,.\, 4)^6$, $F_3 = 3 \,.\, 3^2 + 8^2 = 91$;

therefore $\mathfrak{N} = 91\,(91 - 3 \,.\, 8 \,.\, 3)(91 + 3 \,.\, 8 \,.\, 3) = 91 \,.\, 19 \,.\, 163$; and $N = \mathfrak{N}$.

15. *Higher Order Forms* ($k > 2$).—It should be understood that—although (for the sake of brevity) the detail of only the simpler cases (when $k = 2$, $j = \pm 1$, and $k = 3$, $j = -1$) has been entered into—the process is applicable to forms of *any* order (k). And the proposed number N will usually be resolvable into the ***same number*** of algebraic factors as the *derived* $\mathfrak{N}$ possesses, excepting only those *lost* under Rules (8*b*), (9*b*). Thus, when $\mathfrak{N}$ has the simplest form (11), it has always at least *two* algebraic factors (except when $j = -1$, and $k = 2^\epsilon$, $\epsilon > 0$), and has *more than two* when k is composite (except when $j = -1$, and $k = 2^\epsilon$, or $2^\epsilon . q$, q being an odd prime, and $\epsilon > 0$), the number of factors usually increasing with the degree of compositeness of k; and these algebraic factors may themselves—under suitable conditions—be susceptible of an *Aurifeuillian** resolution.

Example, of a very large number with binomial forms of 15th order ($k = 15$).

Given $N = \Phi_{15} = \Phi'_{15}$; $\Phi_{15} = \mu \,.\, 1^{15} + \nu \,.\, 9^{15}$, $\Phi'_{15} = \mu \,.\, 4^{15} + \nu \,.\, 5^{15}$;

where $\mu = 4 \,.\, 41 \,.\, 541 \,.\, 45061$, $\nu = 9 \,.\, 7 \,.\, 331$, $k = 15$;

Here $D = \dfrac{4^{15} - 1^{15}}{\nu} = \dfrac{9^{15} - 5^{15}}{\mu} = 11 \,.\, 31 \,.\, 151$; $\mathfrak{N} = (4 \,.\, 9)^{15} - (1 \,.\, 5)^{15}$;

then $\mathfrak{N}$ is resolvable (algebraically) into *four* factors, since $k = 3 \,.\, 5$; say

$$\mathfrak{N} = F_1 \,.\, F_3 \,.\, F_5 \,.\, F_{15};$$

where $F_1 = 36^1 - 5^1$, $F_3 = \dfrac{36^3 - 5^3}{36^1 - 5^1}$, $F_5 = \dfrac{36^5 - 5^5}{36^1 - 5^1}$, $F_{15} = \dfrac{F'_{15}}{F_5}$, $F'_{15} = \dfrac{36^{15} - 5^{15}}{36^3 - 5^3}$;

then $F_1 = 31$; $F_3 = 1501 = 19 \,.\, 79$;

also F_5, F'_{15} are both *Quint-Aurifeuillians*,† and are therefore resolvable by the Aurifeuillian resolution into *two* large factors each, as follows :—

$$F_5 = (36^2 + 3 \,.\, 36 \,.\, 5 + 5^2)^2 - 5 \,.\, 5 \,.\, 36\,(36 + 5)^2 = 1861^2 - 1230^2 = (631)(11 \,.\, 281):$$

$${}'_{15} = (36^6 + 3 \,.\, 36^3 \,.\, 5^3 + 5^6)^2 - 5 \,.\, 5^3 \,.\, 36^3 (36^3 + 5^3)^2 = 2194293961^2 - 252617400^2$$

$$= (1941676561)(2446911361), \quad [\text{which contains } F_5].$$

---

* See the author's paper "On Aurifeuillians" above quoted.

† *I.e.*, Aurifeuillians of the fifth order: see the author's paper "On Aurifeuillians" quoted, and Ed. Lucas's paper "Sur la série récurrente de Fermat," Rome, 1879, p. 6.

$$F_{15} = \frac{F'_{15}}{F_5} = \frac{1941676561}{11 . 281} . \frac{2446911361}{631} = 628171 . 3877831 = (628171)(61 . 151 . 421);$$

$$N = \frac{\mathfrak{N}}{D} = \frac{F_1 . F_3 . F_5 . F_{15}}{D} = \frac{(31)(19 . 79)\{(631)(11 . 281)\}\{(628171)(61 . 151 . 421)\}}{11 . 31 . 151}$$

$$= (19 . 79)\ \{(631)(281)\}\{(628171)(61 . 421)\}\ ;$$

here the given number N has been resolved *algebraically* into *five* factors (shown inside the brackets); one of the *six* algebraic factors of $\mathfrak{N}$ having been lost on division by D.

16. *Condition of Factorisability.*—It will be seen that when the derived $\mathfrak{N}$ is resolvable into *two* factors ($\mathfrak{N} = L . M$) then the proposed N is also always resolvable into *two* factors under a certain condition (8*b*) which may be expressed

Provided neither of L, $M = D$, or $=$ a factor of D, (59*a*)

and when $\mathfrak{N}$ is resolvable into *three* factors ($\mathfrak{N} = L_1 . L_2 . L_3$), then N is also always resolvable into *three* factors under a similar condition (9*b*) which may be expressed

Provided neither of L_1, L_2, $L_3 = D$, or $=$ a factor of D. (59*b*)

There is one case in which this condition (59*a*, *b*) can be seen to be satisfied *a priori* (*i.e.*, before attempting to resolve $\mathfrak{N}$) viz.,

When $D = 1$, then $N = \mathfrak{N}$, and the factorisation of $\mathfrak{N}$ involves that of N. (60)

Another case in which the condition is satisfied can sometimes be recognised *a priori*, viz.,

When D is so small as to be obviously $<$ both L, M, then the factorisation of $\mathfrak{N}$ involves that of N. (60*a*)

The general condition in (59*a*, *b*) is an *a posteriori* condition, *i.e.*, its applicability is not recognisable until *after* the factorisation of $\mathfrak{N}$ has been effected; the two special forms (60), (60*a*) are probably as convenient as can be expected. The general form and both the special forms involve in general all the coefficients (μ, ν, μ', ν'), and also all the elements (x, y, x', y') entering into the twin forms (Φ_k, Φ'_k).

It is much to be wished that some *a priori* form of the general condition (59*a*, *b*) could be found. At present this has been done (so far as known to the author) for two quadratic forms only (Art. **8**, **12**).

Isomorph Quadratics (Φ_2, Φ'_2). Φ_2, Φ'_2 must *not be Automorphs.* (61*a*)

Conformal Quadratics (Φ_2, Φ'_2). Φ_2, Φ'_2 must *not be Automorphs.* (61*b*)

The mode of expressing the *general* condition used in (10) is suggested as probably a suitable expression of it, viz.,

$$\text{The twin forms } \Phi_2,\ \Phi_2' \text{ must be } \textit{non-equivalent}, \tag{62}$$

where the term *equivalent* may be taken to mean *interchangeable by some algebraic process.*

[The discovery of such a condition is perhaps more of theoretic than of *practical* interest; as it seems quite likely that the application of such a condition might be more troublesome than the attempt at factorisation itself.]

A Geometrical Theory of Differential Equations of the First and Second Orders. *By* R. W. H. T. Hudson. Received January 28th, 1901. Communicated February 14th, 1901.

1. *Introduction.*

The differential equations dealt with in this paper are ordinary and of the first and second orders. The variables are regarded as real, so that the usual geometrical interpretation and terminology can be employed throughout.

The main ends towards which the investigation is directed are to find conditions that a differential equation of the second order of general algebraic form may have singular solutions of the various kinds which are possible, and to examine their relations to other solutions. Since the singular solutions, if they exist, satisfy an equation of the first order, it is necessary to enter upon a preliminary investigation of these equations, and, in particular, to find the conditions that a singular solution may represent an osculating envelope. This occupies the second section; the method chiefly employed is geometrical, and the results are obtained by projection from figures in space of three dimensions. For completeness and greater generality the unspecialized form of equation is first discussed, and the usual results are obtained very simply in this manner.

In the third section the same method is employed to examine solutions of equations of the second order, and the results of the preceding section are frequently applied. In some cases it is simpler to integrate the given equation by means of series of which the leading terms are found by the use of a diagram of unit points. In all cases the method adopted is that which seems to lead to the desired result in the shortest manner. The same results may, of course, be obtained by more straightforward, but much longer, processes. In particular, the various possibilities of loci contained in the discriminant of a discriminant may be worked out as a piece of algebra, and will be found to amount to the same as those which are obtained by geometrical intuition.*

In the following pages the theory is regarded from the point of view of the differential equation, not the complete primitive. As has been pointed out by Darboux, Cayley, and others, the theories are distinct, and what occurs as a general rule in one case must be regarded as exceptional in the other. But, before proceeding, a few remarks may be made on the theory of the complete primitive, as most writers have dealt with the subject from this point of view, and some of their results can be obtained very shortly by considerations analogous to those employed in the latter sections of this paper.

The subject may be said to have been started by Cayley in his paper† "On the Theory of the Singular Solutions of Differential Equations of the First Order." The type of differential equation considered is integrable, and corresponds to a system of curves represented by

$$f(x, y, c) = 0,$$

where c is either one parameter or stands for m parameters connected by $m-1$ algebraic relations. Cayley proves that the c-discriminant locus is made up of the envelope, nodal and cuspidal loci, and that the p-discriminant locus consists of the cuspidal locus, tac-locus, and envelope; and states without proof the number of times each occurs. A singular solution is defined as belonging to the envelope species, and from this definition it is deduced that the singular solution must satisfy not only the differential equation

$$\phi = 0,$$

but also the derived equation

$$\frac{\partial \phi}{\partial p} = 0;$$

---

* This has been done by Prof. Henrici in Vol. II. of the *Proc. Lond. Math. Soc.*, 1868, p. 104 and p. 177.

† *Mess. of Math.*, 1873, Vol. II., p. 6.

but it may happen, as will be seen later, that the curve representing a common solution is not an envelope.[*]

In a later paper bearing the same title,[†] Cayley proves that two neighbouring curves of an algebraic system cut one another in points at which the tangents are nearly coincident, the number of such points being equal to the sum of the order and class of the curves, a necessarily positive number, whence the conclusion that an algebraic system of curves always has an envelope;[‡] on the other hand, it is pointed out that in general no part of the p-discriminant provides a solution of the differential equation. Cayley remarks that it at once appears by drawing consecutive curves with nodes and cusps that two ultimate intersections coincide at a node and three at a cusp, whence, doubtless, he was able to infer the number of times these loci occur in the c-discriminant locus.

When the complete primitive involves only one constant c, we may take $c = z$ to be a third coordinate. This is suggested by Cayley, who, however, does not apply the conception. Prof. Hill[§] points out that the node-locus and cusp-locus can be regarded as projections of a nodal line and cuspidal line on a surface, and uses this idea to illustrate his theorems about the directions of tangents at nodes and cusps on curves of the family.

The consideration of this surface leads at once to the connection between the number of times the factors of the c-discriminant are repeated and the coefficients of δ and κ in Plücker's formula for the class of any curve. For the order of a circumscribing cone is the class of a section of the surface by a plane passing through the vertex. Now, if n is the order of the surface

$$f(x, y, z) = 0,$$

the order of the z-discriminant is

$$n(n-1), \quad = m + 2\delta + 3\kappa,$$

---

[*] In Vol. L. of the *Math. Annalen*, p. 103, M. Petrovitch shows that the differential equations

$$f(x, y, y') = 0, \quad \partial f/\partial y' = 0$$

may have a common solution which is not an envelope of integral curves of the equation $f = 0$, and that this is due to the vanishing at every point of the locus obtained of other derivatives of f with respect to y and y'.

[†] *Mess. of Math.*, 1877, Vol. VI., p. 23.

[‡] Prof. Chrystal points out that these ultimate intersections may be the same for all the curves, in which case there is no true envelope. *Edin. Phil. Trans.*, Vol. XXXVIII., 1896, p. 803.

[§] *Proc. Lond. Math. Soc.*, 1888, Vol. XIX., p. 565.

where m is the class of any section and the order of the circumscribing cylinder whose generators are parallel to the axis of z, and δ, κ are the orders of the nodal and cuspidal lines. The section of the z-discriminant cylinder by any plane parallel to the axis of z consists of $n(n-1)$ parallel straight lines of which m are isolated, 2δ coincide in pairs and pass through the δ nodes of the section of f, and 3κ coincide in threes and pass through the κ cusps of the section of f. Hence the z-discriminant has the form

$$EN^2C^3,$$

where $E = 0$ is the envelope of

$$f(x, y, c) = 0,$$

$N = 0$ is the node-locus, and $C = 0$ is the cusp-locus. Since the same formula holds good for curves possessing higher singularities when these are replaced by their "equivalent" nodes and cusps, the number of times the locus of these points occurs in the discriminant locus may be inferred.

Two theorems proved by Prof. Hill follow at once from the geometrical conception just considered.* The theorems are

(1) If $\partial^2 f/\partial c^2 = 0$ at all points of the node-locus, this is also an envelope, and N^3 is a factor of the discriminant.

(2) If $\partial^2 f/\partial c^2 = 0$ at all points of the cusp-locus, this is also an envelope, and C^4 is a factor of the discriminant.

The node-locus is the projection of a nodal line on the surface

$$f(x, y, z) = 0,$$

and at every point of the nodal line

$$f_x = 0, \quad f_y = 0, \quad f_z = 0,$$

and the quadratic form

$$(f_{xx}, f_{yy}, f_{zz}, f_{yz}, f_{zx}, f_{xy})\!(X-x, \; Y-y, \; Z-z)^2$$

breaks into two distinct factors. If now

$$f_{zz} = 0,$$

one of the factors must be

$$f_{xz}(X-x)+f_{yz}(Y-y),$$

---

* "On Node- and Cusp-Loci which are also Envelopes," *Proc. Lond. Math. Soc.*, 1891, Vol. xxii., p. 216.

which means that one of the tangent planes at every point of the nodal line is parallel to the axis of z. Thus, considering each sheet of the surface separately, we see that the nodal line is projected on to the plane $z = 0$ as the envelope of the projections of the sections of one sheet by planes perpendicular to the axis of z. Further, if we consider the distribution of lines parallel to the axis of z lying in any plane and satisfying the z-discriminant equation, we find that three coincide at every intersection of the nodal line and this plane; in fact, there are only $m-\delta$ isolated lines in this case, and the discriminant must contain N^3 as a factor.

In the case of a cuspidal edge the two factors of the quadratic form are the same; so that the condition

$$f_{zz} = 0$$

involves the relations $\quad f_{xz} = 0, \quad f_{yz} = 0,$

and then the repeated tangent plane is given by

$$(f_{xx}, f_{xy}, f_{yy} \between X-x, Y-y)^2 = 0.$$

The projection of the edge is an envelope of projections of sections of both sheets; but these sections meet in pairs on the edge and form cusps there. Hence the projection of the edge is an enveloping cusp-locus. Considerations similar to those applied to the node-locus show that C^4 must be a factor of the discriminant.

2. *Equations of the First Order.*

Considerable clearness may be introduced into the theory of ordinary differential equations of the first order by the use of an idea suggested by Poincaré.* The usual geometrical interpretation of an equation

$$f(x, y, y') = 0 \quad \left(y' \equiv \frac{dy}{dx}\right)$$

is to make it associate one or more directions y' with each point (x, y) of a plane. In this way "integral curves" are obtained, such that each of the directions associated with any point is the tangent to an integral curve through that point.

The geometrical interpretation which is here described and developed consists in regarding y' as the the third coordinate z of a point (x, y, z) in space. Then, to any curve α in the plane of x, y corresponds a space-curve β of which α is the orthogonal projection, and the distance between any point on β and its projection on α is equal to the tangent of the angle made by the tangent to α with the axis of x.

---

* *Journal de Math.*, 1885, sér. 4, t. I., p. 196; see also Lie-Scheffers, *Geometrie der Berührungs-Transformationen*, 1896, pp. 182–191.

The chief convenience of this representation is that the condition that two curves α *touch* is the same as that the corresponding curves β *cut* one another; and, more generally, the condition that two curves α have contact of the n-th order is the same as that the corresponding curves β have contact of the $(n-1)$-th order.

To the equation $\quad f(x, y, y') = 0$

corresponds the surface $\quad f(x, y, z) = 0,$

and to the integral curves in the plane $z = 0$ correspond curves on the surface $f = 0$, for which

$$dy - z\,dx = 0.$$

For convenience, let the integral curves be called *α-curves* and their space representatives *β-curves*. Then, through any point (x, y, z) on the surface $f = 0$ passes one β-curve, its direction being given by the intersection of the tangent plane

$$(X-x)\frac{\partial f}{\partial x} + (Y-y)\frac{\partial f}{\partial y} + (Z-z)\frac{\partial f}{\partial z} = 0,$$

and the plane $\quad z(X-x)-(Y-y) = 0.$

Suppose that the axis of z is drawn vertically upwards. The latter plane is then a vertical plane and cuts the former in a determinate line, except in the special case when the two planes coincide.

If the α-curves have an envelope, then through a point of the plane $z = 0$ near the envelope pass two α-curves whose directions are nearly the same. Corresponding to them in space we have two β-curves cutting a vertical line in two near points. We infer that the vertical cylinder standing on the envelope circumscribes the surface $f = 0$ on which the β-curves lie.

We should therefore consider in general the relation between the curve of contact of the vertical circumscribing cylinder and the β-curves. The curve of contact, which will be called C, is given by the equations

$$f(x, y, z) = 0,$$

$$\frac{\partial f}{\partial z} = 0,$$

and the circumscribing cylinder is found by eliminating z.

The direction of the β-curve through any point of C is given, in general, by the intersection of the two vertical planes

$$(X-x)\frac{\partial f}{\partial x} + (Y-y)\frac{\partial f}{\partial y} = 0,$$

$$(X-x)z - (Y-y) = 0;$$

that is to say, all the β-curves have vertical tangents at the points where they cross C.

Now, as a variable point moves along β and passes through a position where the tangent is vertical, the projection which describes a passes through a position in which it is stationary; that is, a has a stationary point, or cusp. This is intuitively obvious when the surface has a general form.

We thus obtain without calculation the known result that, *in general, a locus obtained by eliminating* y' *from*

$$f(x, y, y') = 0,$$

$$\frac{\partial f}{\partial y'} = 0,$$

is a cusp-locus for the integral curves of the equation

$$f(x, y, y') = 0.^*$$

---

* [*Note added July*, 1901.—In general there are a certain number of points on C at which $f_x + zf_y = 0$, and the above reasoning breaks down. These correspond to *singular points* of the differential equation. For the shapes of the integral curves at these points see a paper by Dyck in the *Sitzungsberichte d. Akad. d. Wiss. zu München*, 1891, Bd. XXI., p. 23, where carefully drawn figures of the three possible cases are given. It appears that in a whole class of cases the integral curves which have cusps at different points of the discriminant locus touch it elsewhere at one and the same point (a *nœud*). This is illustrated by a particular example given by Prof. Chrystal (*loc. cit.*). In many cases the coefficients in the differential equation can be modified so that it may possess an algebraic primitive without altering the general shape of the integral curves, so that such families of curves form an exceptional class in the general theory of envelopes.]

The reasoning given above applies to any sheet of the surface $f = 0$ which has vertical tangent planes. It is therefore unnecessary to make any special supposition as to the way in which the arguments x, y, y' are involved in $f(x, y, y')$, except that the surface $f(x, y, z) = 0$ must have the properties of an algebraic surface in the neighbourhood of points where the tangent plane is parallel to the axis of z.

The exceptional case occurs when the equations

$$(X-x)f_x+(Y-y)f_y = 0,$$

$$(X-x)z-(Y-y) = 0$$

coincide at all points of C.*

The analytical conditions are that at every point of C the following equations are satisfied:—

$$f(x, y, z) = 0,$$

$$f_x+zf_y = 0,$$

$$f_z = 0,$$

or we may say that the result of eliminating y, z from these three equations must be an identity.

These are the known necessary and sufficient conditions (in the absence of further special relations) that the integral curves of $f(x, y, y') = 0$ may have an envelope, or, what is here the same thing, that the equation

$$f(x, y, y') = 0$$

may have a singular solution. In fact, the curve C satisfies the equation

$$\frac{\partial f}{\partial x}dx+\frac{\partial f}{\partial y}dy = 0,$$

and therefore

$$dy-z\,dx = 0,$$

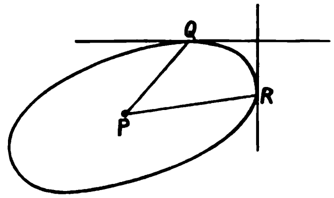
except when f_x and f_y vanish; so that the projection of C is a solution of the differential equation, that is, C represents a singular solution. The exceptional case, to be at present excluded, occurs when C is a double line on the surface.

It remains to be investigated how the β-curves behave in the neighbourhood of C. It is necessary only to take a point Q near C

---

[*] Compare Fine, *Amer. Jour. of Math.*, Vol. XII., p. 302.

and find the direction of the β-curve through it. Through each point of C pass two curves whose plans (projections on $z = 0$) satisfy $f(x, y, y') = 0$; one of these is the curve C itself, corresponding to a singular solution, and the other is a β-curve whose plan is an ordinary integral curve touching the singular solution.



The directions of these curves may be found by the following geometrical construction. Take any point P on C and construct the indicatrix, which will be a small conic in a vertical plane. Draw a vertical tangent line touching at R and a horizontal tangent touching at Q. *Then PR is the direction of C, and PQ that of the β-curve which cuts C at P.* These results can be deduced by simple geometrical reasoning from the definitions of the two curves.

This discrimination between the directions of the two curves on the surface $f(x, y, z) = 0$ at points where every direction in the tangent plane satisfies $dy = z\,dx$ corresponds to the discrimination between the curvatures of the singular solution of $f(x, y, y') = 0$ and the integral curve which touches it at any point. It is easy to verify that at such a point the two values of y'' are the roots of the quadratic equation

$$\frac{d^2 f}{dx^2} = 0,$$

which breaks up into $$\frac{d}{dx}\left(\frac{\partial f}{\partial y'}\right) = 0,$$

giving the curvature of the envelope, and

$$\frac{d}{dx}\left(\frac{\partial f}{\partial y'}\right) + \frac{\partial f}{\partial y} = 0,$$

giving the curvature of the integral curve.

Hitherto only one condition has been imposed upon the surface $f = 0$, namely, that the curve of contact C of the vertical circumscribing cylinder is the same as the unique curve on this cylinder which satisfies $dy = z\,dx$. We proceed to find what further conditions must be satisfied in order that the plan of C may be an *osculating* envelope of α-curves.

In this case the β-curves must touch C; but they cannot cut one another except on C. It is thence intuitively obvious that the parts of a β-curve separated by the point of contact with C are on different sheets of the surface; so that the β-curves are characteristics and C is an edge of regression on the surface $f = 0$. Since two consecutive characteristic β-curves cut one another at each point of C, therefore the tangent plane to the surface there must be the vertical plane

$$z(X-x)-(Y-y) = 0.$$

[The plan of a cuspidal edge is generally an ordinary envelope of plans of characteristics; it is only when the tangent planes are vertical that the plans can cross and so osculate.]

The necessary and sufficient analytical conditions that the line

$$f = 0, \quad f_z = 0$$

may have these properties are that at every point of it

$$f_x = 0, \quad f_y = 0,$$

$$f_{xx} = -zf_{xy} = z^2 f_{yy},$$

$$f_{xz} = 0, \quad f_{yz} = 0, \quad f_{zz} = 0,$$

which are equivalent to

$$\frac{dy}{dx} = z, \quad f_y = 0, \quad f_{yz} = 0, \quad f_{zz} = 0.$$

The horizontal sections of the surface f, *i.e.*, sections by planes $z =$ const., project into the loci of contacts of parallel tangents considered by Prof. Hill.* Since the envelope of these curves is obviously the base of the vertical circumscribing cylinder, the fact that they touch the cusp locus and also the envelope of the integral curves needs no further proof.

The following results have now been obtained:—

(1) The existence of a locus of cusps on α-curves follows generally from the existence of β-curves on the surface f.

(2) The existence of an envelope of α-curves requires a special form of f, but not necessarily the presence of geometrical singularities.

---

* *Proc. Lond. Math. Soc.*, Vol. xix., p. 577.

(3) The existence of an osculating envelope of α-curves requires a cuspidal edge on f with vertical tangent planes.

Assuming next that f possesses singular lines, we proceed to investigate their relations to β-curves and the relations of their plans to α-curves.

Consider a *nodal line*. Let $P(x, y, z)$ be any point on it. In general the plane

$$Y-y = z(X-x)$$

cuts the surface along two distinct directions through P, so that distinct β-curves cross at the point. The plans therefore touch, but are not consecutive. *Hence, in general, the plan of a nodal line is a tac-locus.*[*]

By considering a penultimate form of surface we see that the nodal line counts twice over as part of the curve of contact of the circumscribing cylinder. Hence the known result that the tac-locus occurs as a repeated factor in the y'-discriminant.

Next, impose the condition that the tangent to the nodal line at any point (x, y, z) on it lies in the vertical plane

$$Y-y = z(X-x).$$

The plan of the nodal line is then a solution of the differential equation. To find its relation to α-curves consider separately the two sheets of f which cut along the nodal line. On each is a singly infinite system of β-curves, and the nodal line belongs to both systems. In plan there are two systems of α-curves having a common member, which satisfies both

$$f(x, y, y') = 0$$

and

$$\frac{\partial f}{\partial y'} = 0,$$

but is *not* an envelope of α-curves, and is in fact a particular integral.[†]

In order that the plan of the nodal line may be an envelope, it is necessary that through every point of it a β-curve should pass distinct from the nodal line.

---

[*] This is the locus of nodes on loci of contacts of parallel tangents (see Hill, *Proc. Lond. Math. Soc.*, Vol. xix., p. 584).

[†] For the analytical distinction between particular and singular solutions, see Hamburger, *Crelle*, t. cxii., p. 205, and Forsyth, *Theory of Differential Equations*, Vol. ii., p. 261.

Hence the vertical plane touching the nodal line must touch also one sheet of f. The two sheets may be considered separately, and we find that the line is an ordinary β-curve for one sheet and a curve of contact of the vertical circumscribing cylinder for the other sheet. In plan there are two systems of a-curves, one member of one system being the envelope of the other system.

The analytical conditions for this are found by expressing the fact that the quadric cone

$$(f_{xx} f_{yy} f_{zz} f_{yz} f_{zx} f_{xy} \between X-x,\ Y-y,\ Z-z)^2 = 0$$

breaks up into two planes, one of which is

$$z(X-x)-(Y-y) = 0.$$

Hence
$$f_{zz} = 0,$$
$$f_{xz}+zf_{yz} = 0,$$
$$f_{xx}+2zf_{xy}+z^2 f^{yy} = 0,$$

which are equivalent to

$$\frac{dy}{dx} = z, \quad f_{zz} = 0.$$

Consider next a *cuspidal edge* on f.

In general the plane

$$Y-y = z(X-x)$$

through any point (x, y, z) of the edge cuts the surface in a curve having a cusp at the edge. As we proceed from the cusp along either branch, the initial change in z has the same sign for both branches, except in the special case when the tangent plane is horizontal; therefore the vertical tangent planes to both branches of the β-curve begin to turn in the same direction from their common position at the cusp. Hence the corresponding a-curve, the plan of the β-curve, has a cusp at (x, y), and both branches lie on the same side of the tangent. The a-curve has, therefore, a *rhamphoid cusp.*

In fact, the plane $Y-y = z(X-x)$ is the osculating plane of the β-curve at its cusp, and, since at a stationary point the osculating plane has contact of order higher by one than at an ordinary point, so at a cusp the osculating plane does *not* cross the curve. Therefore, the projection on a plane at right angles to the osculating plane has a rhamphoid cusp.

The edge provides a solution of the differential equation if the plane $Y-y=z'X-x$, touches it. We have then two families of β-curves, one on each sheet of the surface, the edge being a β-curve common to both families. The projection of the edge is then a particular solution, but not an envelope of a-curves.

In order that it may be an envelope, the β-curves must cut the edge. In this case they will have a cusp there unless they also touch the edge; they are then characteristics of the surface. Thus the condition that the plan of the edge may be an envelope of a-curves is sufficient to make it an osculating envelope.

Before proceeding to more special forms of surface and differential equations of higher order it is useful to obtain some of these results in a different manner.

Suppose that a singular solution exists; it is required to find its relation to integral curves and to find what conditions must be satisfied that it may be an osculating envelope.

Let y and z be the functions of x corresponding to the singular solution, z being here $\frac{dy}{dx}$, and let $y+\eta$, $z+\eta'$ correspond to another solution. Then the equation for η is

$$f(x,\ y+\eta,\ z+\eta')=0;$$

or, expanding and using the identities

$$f(x,y,z)=0,\quad f_z=0,$$

this becomes $$\eta f_y+\tfrac{1}{2}\eta^2 f_{yy}+\eta\eta' f_{yz}+\tfrac{1}{2}\eta'^2 f_{zz}+\ldots=0,$$

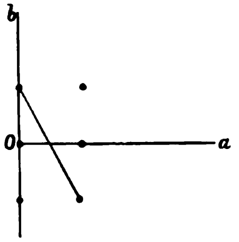
where the coefficients are functions of x and are to be expanded in powers of $x-x_0$, if an expansion for η is required corresponding to initial values

$$x=x_0,\quad \eta=y_0,\quad \eta'=z_0.$$

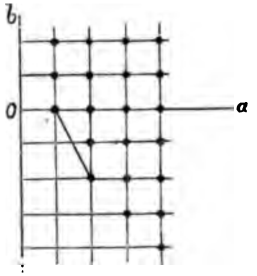
The method of obtaining this expansion is as follows:—* Write ξ for $x-x_0$ and substitute ξ^μ for η; corresponding to any term $\xi^{a\mu+b}$, mark on a diagram the point whose rectangular coordinates are a, b. Join these points to form a polygon, excluding none of them. Then a side nearer to the origin than any internal point determines which terms may be taken together to be of lowest order, and the corresponding value of μ is the tangent (with proper sign) of the inclination of the side to the axis of a. For example, the value of μ for the line represented in the diagram is $+2$.

---

* For an explanation of the application of a Puiseux diagram to differential equations see Fine, *Amer. Jour. of Math.*, Vol. XI., p. 317, and Briot et Bouquet, *Jour. Polyt.*, Cah. XXXVI., where the horizontal axis is taken one place lower than in the present paper.



To construct the diagram for the differential equation for η we have to mark, corresponding to the term $\frac{1}{m!\,n!}\eta^m\eta'^n\frac{\partial^{m+n}f}{\partial y^m\partial z^n}$, the point $(m+n,\ -n)$ and all unit points having the same abscissa and greater ordinates. But to obtain the sides of the polygon it is necessary to mark only the *lowest* point on each column; so it is unnecessary to expand $\frac{\partial^{m+n}f}{\partial y^m\partial z^n}$ in powers of ξ.



Now we are concerned only with values of μ greater than unity, because we want an expansion for an integral curve which touches the singular solution. A glance at the diagram shows that the terms

$$\eta f_y \quad \text{and} \quad \tfrac{1}{2}\eta'^2 f_{zz}$$

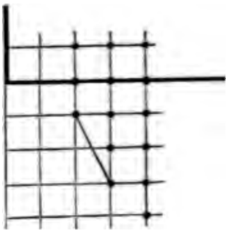
may be taken together. and give

$$\eta = -\tfrac{1}{2}\,(f_y/f_{zz})\,\xi^2+\dots,$$

showing that the second derivatives of the dependent variable corresponding to the singular solution and integral curve differ by f_y/f_{zz}, as indicated before (p. 388).

If we suppose that f_y vanishes at all points of the solution, as is the case when the corresponding line on the surface $f(x, y, z) = 0$ is a singular line, then the first column of points disappears from the diagram, and the new polygon has no side for which μ is greater than unity. Thus no integral curve touches the solution at any point of it; so that the solution is, in this case, not an envelope, but a particular solution.

To make it an envelope we must arrange that the point $(2, -2)$ may disappear. This is effected by supposing that f_{zz} vanishes at all points of the solution. We have now satisfied the conditions which



make one set of tangent planes at the nodal line on

$$f(x, y, z) = 0$$

vertical. The diagram shows that the terms

$$\eta\eta' f_{yz} + \tfrac{1}{6}\eta'^3 f_{zzz}$$

may be taken to give

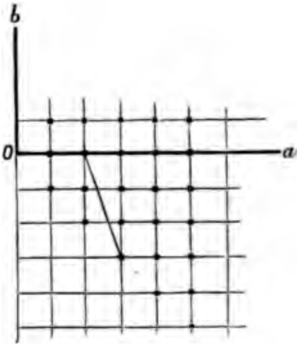
$$\eta = -\tfrac{3}{2}(f_{yz}/f_{zzz})\,\xi^2 + \dots;$$

so that the second derivatives differ by $3(f_{yz}/f_{zzz})$.

In order that the singular solution may be an osculating envelope, one side of the polygon must give $\mu = 3$. This requires that the point (2, −1) must disappear, or f_{yz} must vanish. [This corresponds to the case of a cuspidal edge on $f(x, y, z) = 0$ with vertical tangent planes.]

Hence the conditions that at every point of a solution of $f(x, y, y') = 0$ the following relations hold, namely,

$$\frac{\partial f}{\partial y} = 0, \quad \frac{\partial f}{\partial y'} = 0, \quad \frac{\partial^2 f}{\partial y\,\partial y'} = 0, \quad \frac{\partial^2 f}{\partial y'^2} = 0,$$



are sufficient to make that solution an osculating envelope of other solutions; and these conditions are also necessary because it is impossible to retain any of the corresponding points, namely, (1, 0), (1, −1), (2, −1), (2, −2), and at the same time have a side of the polygon inclined at an angle $\tan^{-1} 3$ to the axis of a.*

These conditions may cease to be sufficient when other derivatives of f vanish; for instance, if, in addition,

$$\frac{\partial^3 f}{\partial y'^3} = 0,$$

causing the point (3, −3) to disappear, the only value of μ obtainable from the diagram is 2, and hence the envelope cannot be osculating.

3. *Equations of the Second Order.*

The integral curves and singular solutions of the differential equation of the second order

$$F(x, y, y', y'') = 0$$

---

* With the points (1, 0), (1, −1) disappear also all the other points of the first column.

can be investigated in a geometrical manner by considering the space curves defined by

$$dx = \frac{dy}{z} = \frac{dz}{w},$$

where w is the function of x, y, z given by

$$F(x, y, z, w) = 0.$$

These curves will be called *γ-curves*.

Assume that F is a polynomial in its arguments and of degree n in w. Then, through every point (x, y, z) pass n curves whose tangents lie in the same vertical plane

$$Y-y = z(X-x).$$

If $\Delta(x, y, z)$ is the w-discriminant of F, then the surface $\Delta = 0$ has the property that of the n γ-curves passing through any point of it two have the same tangent.

The direction cosines of the osculating plane at any point of a γ-curve are proportional to the determinants

$$\begin{Vmatrix} dx & dy & dz \\ d^2x & d^2y & d^2z \end{Vmatrix}$$

or

$$\begin{Vmatrix} 1 & y' & z' \\ 0 & y'' & z'' \end{Vmatrix}$$

or

$$\begin{Vmatrix} 1 & z & w \\ 0 & w & \frac{dw}{dx} \end{Vmatrix}$$

or

$$z\frac{dw}{dx} - w^2, \quad -\frac{dw}{dx}, \quad w.$$

Now

$$\frac{dw}{dx} = -\left(F_x + F_y\frac{dy}{dx} + F_z\frac{dz}{dx}\right)\Big/ F_w;$$

so that, at an ordinary point of Δ,

$$\frac{dw}{dx} = \infty.$$

The osculating plane is then normal to the direction

$$z, \quad -1, \quad 0,$$

and is therefore the vertical plane

$$z(X-x)-(Y-y)=0.$$

The meaning of $$\frac{dw}{dx}=\infty \quad \text{or} \quad \frac{d^2z}{dx^2}=\infty$$

is that the γ-curve has a cusp, and since the osculating plane is vertical, the plan has a rhamphoid cusp (see p. 391). Further, through (x, y, z) on Δ passes one "β-curve" defined by $dy = z\,dx$; and the plan of this curve (projection on $z = 0$) touches the plan of the γ-curve at the cusp. We have therefore proved that *the solutions of the equation* $\Delta(x, y, y') = 0$ *are tangent loci of rhamphoid cusps on integral curves of the equation* $F(x, y, y', y'') = 0$.*

For convenience we shall call integral curves of the equations

$$\Delta(x, y, y') = 0, \quad \text{and} \quad F(x, y, y', y'') = 0,$$

Δ-curves and *F-curves* respectively; so that Δ-curves are plans of β-curves and correspond to the α-curves of the previous work, and F-curves are plans of γ-curves.

Let $\phi(x, y, z)$ be the coefficient of w^n in $F(x, y, z, w)$. Then at every point of the surface $\phi = 0$ one value of w is ∞. For the corresponding γ-curve $\frac{dz}{dx} = \infty$; so that the tangent is vertical, and therefore the plan has an ordinary cusp. Thus the integral curves of the equation

$$\phi(x, y, y') = 0$$

are tangent loci of ordinary cusps on integral curves of

$$F(x, y, y', y'') = 0.*$$

A certain number of F-curves can be drawn through each point (x, y) in any direction determined by y'. The meaning of the equation

$$\Delta(x, y, y') = 0$$

is that two of these curves have the same y'', that is, the same curvature. The following cases are *a priori* possible:—

(1) The curves are branches of the same F-curve, and together form a rhamphoid cusp.

(2) The curves are distinct F-curves.

(3) The F-curves form a sequence in which each may be said to

---

* This proposition is obtained by Goursat, *Amer. Jour. of Math.*, Vol. XI., p. 364.

touch the next. The envelope is an osculating envelope and a singular solution.

These three cases correspond in a sense to the (1) cusp-locus, (2) tac-locus, (3) singular solution, which may exist in the case of an equation of the first order.

Case (1) has already been examined. The line-elements (x, y, y') considered unite to form the singly infinite system of Δ-curves.

Case (2) occurs when the corresponding γ-curves are distinct and touch. Then $\frac{dw}{dx}$ is not infinite for either curve at the point of contact, and therefore the equation

$$F_x + zF_y + wF_z = 0$$

must be satisfied. This defines a curve Q on Δ. Thus, in general, two distinct F-curves osculate each other at all points of a curve (the plan of Q) obtained by eliminating z, w from

$$\begin{aligned} F(x, y, z, w) &= 0, \\ F_w &= 0, \\ F_x + zF_y + wF_z &= 0. \end{aligned}$$

Further, the value of $\frac{dz}{dx}$ for a β-curve is given by

$$F_x + zF_y + \frac{dz}{dx} F_z = 0,$$

since

$$F_w = 0;$$

so that at all points of Q the tangent γ-curves are touched by a β-curve, or, in other words, the two γ-curves which touch one another touch also the surface Δ. Hence, also, the pair of F-curves which osculate each other at any point of the plan of Q are osculated by a Δ-curve at that point.*

Case (3) occurs when a family of γ-curves has an envelope lying on Δ. This envelope must be a β-curve or else correspond to a solution of

$$\Delta(x, y, y') = 0,$$

---

* [*Note added July*, 1901.—This is a locus of essential singularities, and at each point of it there may be an infinite number of F-curves having contact of the third order with one of the pair discussed above. A detailed examination of the various cases must be reserved for another occasion.]

and, in either case, since it is touched by y-curves, it must be determined by the condition for Q, with the added condition

$$dy = z\,dx.$$

Singular Solutions.[*]

A singular solution of the *first kind* is defined as a solution of

$$\Delta(x, y, y') = 0,$$

which is not a singular solution of this equation, and which satisfies the equation
$$F(x, y, y', y'') = 0.$$

If one exists, it is contained in the locus obtained by eliminating z, w from

$$F(x, y, z, w) = 0,$$
$$F_w = 0,$$
$$F_x + zF_y + wF_z = 0,$$

and is an osculating envelope of F-curves. Since, in general, the values of y and z obtained from these equations do not satisfy

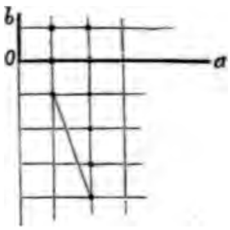
$$dy = z\,dx,$$

so, as in the case of equations of the first order, the existence of a singular solution is exceptional.

To examine the F-curves which osculate a singular solution, we have to solve the equation for η,

$$F(x,\ y+\eta,\ z+\eta',\ w+\eta'') = 0,$$

where y, z, w are the functions of x corresponding to the singular solution. A diagram can be constructed as on p. 393 and shows that the terms of lowest order are



$$\eta' F_z + \tfrac{1}{2}\eta''^2 F_{ww},$$

whence $\eta = -\tfrac{1}{6}(F_z/F_{ww})\,\xi^3 + \dots$;

and therefore the values of y''' for the singular solution and integral curve differ by F_z/F_{ww}.

If all the Δ-curves are singular solutions of $F = 0$, then every

---

[*] See Forsyth, *Theory of Differential Equations*, Vol. II., 1900, pp. 251, 253.

β-curve is touched by γ-curves. The curve Q does not exist; so that the equation

$$F_x + zF_y + wF_z = 0$$

must be an algebraic consequence of $F = 0$, $F_w = 0$. Since w, the common root of the equations in w, $F = 0$, $F_w = 0$ is not infinite at the curve of contact C of the vertical cylinder circumscribing Δ, therefore $\frac{dz}{dx}$ for the γ-curves and β-curves at any point of C is not infinite; that is, the tangent line is not vertical. Hence, when all the Δ-curves are singular solutions of $F = 0$, they have an envelope, the plan of C. It will be proved that this envelope is obtained by eliminating w, z from

$$F = 0, \quad F_w = 0, \quad F_z = 0,$$

and therefore, at every point of it, the osculating Δ-curve and F-curve have the same value for y'''.

A singular solution of the equation

$$\Delta(x, y, y') = 0$$

which satisfies

$$F(x, y, y', y'') = 0$$

is called a singular solution of the *second kind* for the latter equation. As it must be contained in the z-discriminant of $\Delta(x, y, z)$, we must find what loci are included in this and examine their relations to F-curves.

First, consider the surface

$$\Delta(x, y, z) = 0.$$

It is the envelope of the surface

$$F(x, y, z, w) = 0,$$

in which w is regarded as a parameter. Thus, Δ is generated by characteristics[*] which are the ultimate intersections of two near surfaces F, and the characteristic corresponding to any value of w is given by

$$F = 0,$$
$$F_w = 0.$$

The surface Δ has a vertical tangent plane where any surface F which touches it has a vertical tangent plane at some point on the curve of contact. Hence the curve of contact C of the cylinder with vertical generators circumscribing Δ is obtained by eliminating w from

---

[*] Monge, *Application de l'Analyse à la Géometrie.*

$$F=0,\quad F_w=0,\quad F_z=0.$$

Now Δ has a singular line, the locus of points where two characteristics cut. The intersecting characteristics may be either consecutive or distinct. In the former case the line is a cuspidal edge given by the equations

$$F=0,\quad F_w=0,\quad F_{ww}=0,$$

and in the latter case a nodal line given by the conditions, equivalent to two independent conditions, that the equation in w, $F=0$, has two distinct pairs of equal roots.*

Thus the y'-discriminant of

$$\Delta(x, y, y')=0$$

contains three possibilities, and we must examine in turn the relation between γ-curves and

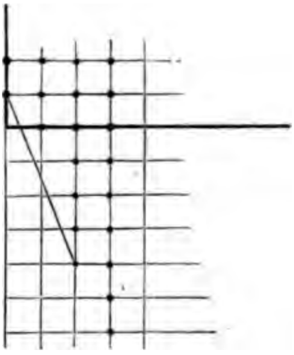
(1) the curve C on Δ,

(2) the nodal line on Δ,

(3) the cuspidal edge on Δ.†

(1) C has no special relation to γ-curves; that is, at each point of C two γ-curves unite to form a rhamphoid cusp, just as at every other point of Δ. This may be seen by integrating the differential equation

$$F(x+\xi,\ y+z\xi+\tfrac{1}{2}w\xi^2+\eta,\ z+w\xi+\eta',\ w+\eta'')=0,$$



where x, y, z, w are now *constants* satisfying

$$F(x, y, z, w)=0,\quad F_z=0,\quad F_w=0,$$

and η is to be obtained as an expansion in powers of ξ in which the leading index is greater than 2. The diagram shows that the terms

$$\xi(F_x+zF_y)+\tfrac{1}{2}\eta''^2F_{ww}$$

are of lowest order, and therefore

$$\eta=\tfrac{4}{15}\left[-2(F_x+zF_y)/F_{ww}\right]^{\frac{1}{2}}\xi^{\frac{5}{2}}+\dots;$$

---

* See p. 269.

† These results are obtained algebraically by Prof. Henrici in Vol. II., *Proc. Lond. Math. Soc.*, 1868, pp. 104 and 177.

so that the expansion for the integral curve is of the form

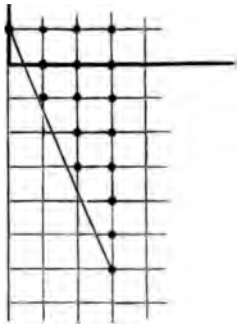
$$y+z\xi+\tfrac{1}{2}w\xi^2+A\xi^{\frac{5}{2}}+\ldots,$$

which is characteristic of a rhamphoid cusp. It is evident from the diagram that the absence of the point (1, −1) corresponding to the term $\eta' F_z$ has not affected the order of the leading term in the expansion for η.

(2) The nodal line is doubly a locus of cusps on γ-curves, one set of cusps corresponding to each sheet. At any point the osculating plane is vertical and the tangents to the two cusps are distinct. In plan we have a line which is a tac-locus for Δ-curves, and at each point are two rhamphoid cusps on F-curves touching the Δ-curves.

(3) This case is best dealt with in plan. We have to integrate, subject to the initial conditions

$$F'=0, \quad F_w=0, \quad F_{ww}=0.$$



The point (2, −4) has now disappeared, and the terms of lowest order are

$$\xi\,(F_x+zF_y+wF_z)+\tfrac{1}{6}\eta''^3\,F_{www},$$

indicating an expansion in which the leading index is $\frac{7}{3}$. The F-curve has a singular point at which three branches osculate each other. But only one can be real; its curvature is finite and the singularity not apparent. It has already been shown that the tangent at the singular point is the tangent at a rhamphoid cusp on a Δ-curve.

If the equation $\quad F(x, y, y', y'')=0$

has a singular solution of the second kind, it must be one of the preceding three loci. We must, therefore, suppose in turn that the curves (1), (2), (3) on Δ satisfy $d_z = w\,dx$ as well as $dy = z\,dx$. It is, however, simpler to consider the plans of these curves, and, assuming them to be solutions of $F=0$, to investigate other solutions which osculate them. The diagram method is now applicable.

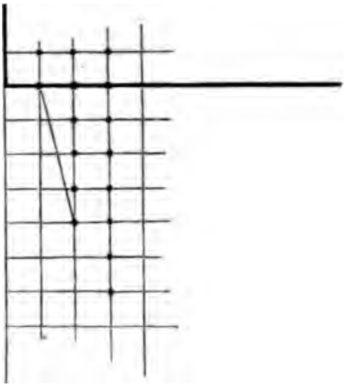
(1) Suppose that the locus obtained by eliminating z, w from

$$F(x, y, z, w)=0, \quad F_z=0, \quad F_w=0$$

is a solution of $\quad F(x, y, y', y'')=0.$

We have to integrate the equation for η

$$F(x, y+\eta, z+\eta', w+\eta'')=0,$$



where y, z, w are the values of y, y', y'' corresponding to the assumed singular solution. The terms of lowest order are

$$\eta F_y + \tfrac{1}{2}\eta''^2 F_{ww};$$

so that the leading index in the expansion of η in powers of ξ is 4. We infer that the F-curve which osculates this singular solution at any point has the same value for y'''.

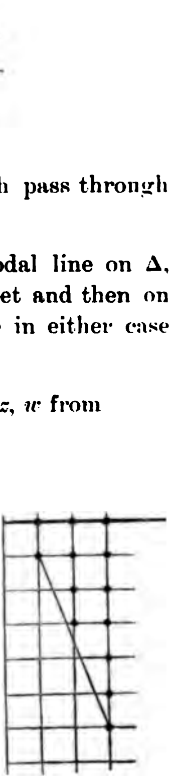
Hence, when the curve C on Δ provides a singular solution of both equations, it is osculated by one of the γ-curves which pass through any point of it.

(2) It is unnecessary to consider further the nodal line on Δ, because it can be treated as a β-curve first on one sheet and then on the other, and the properties which its plan may have in either case must simply be combined.

(3) Suppose that the locus obtained by eliminating z, w from

$$F = 0, \quad F_w = 0, \quad F_{ww} = 0$$

is a solution of $\qquad F(x, y, y', y'') = 0.$



Then, constructing a diagram as before, we find that the points corresponding to F_z and F_{www} indicate an expansion for η in which the leading index is $\frac{5}{2}$. Thus the locus (which is not an envelope of Δ-curves) is an osculating envelope of rhamphoid cusps on F-curves.

We infer that the corresponding γ-curves have cusps touching the cuspidal edge on Δ.

Lastly, we suppose that singular solutions of both kinds exist. The Δ-curves then have an osculating envelope which, as we have seen, must be the plan of the cuspidal edge on Δ when this has vertical tangent planes at every point. Since these planes are also tangents to surfaces F, we have the condition

$$F_z = 0.$$

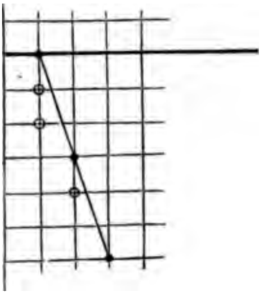
Hence, if the equations

$$F = 0, \quad F_w = 0, \quad F_{ww} = 0, \quad F_z = 0$$

can be solved for y, z, w, and if the functions of x so obtained satisfy

$$dy = z\,dx, \quad dz = w\,dx,$$

then the corresponding locus is a singular solution of the second kind, and is an osculating envelope of singular solutions of the first kind.



That these conditions are necessary in order that both kinds of singular solution may exist appears from the diagram; for the side of the polygon nearest the origin must indicate *two* expansions with leading index 3.

APPENDIX (*a*).

(Session 1900–1901.)

In the list of exchanges, No. 56 (p. 3) should be deleted, as the copy in question is given to the College by a member of the Society.

At the December meeting the Treasurer declined to have a resolution passed for the adoption of his report. The Auditor was thanked for his services by letter from the Secretary.

Mr. J. H. Michell sends the following remarks for insertion in the Appendix :—

There is an oversight in § 3 of my paper "On Transmission of Stress, &c." (*Proc.*, Vol. xxxi., p. 183), which perhaps ought to be pointed out.

The method proposed implies the continuity of the functions $(\lambda+3\mu)\,\theta-2\mu w'_z$, ϖ, &c., across the boundary between the parts of $z=0$, over which the different conditions hold. This continuity will not in general exist. Cases (*c*), (*d*) are covered by Boussinesq's solution, as I have pointed out. The difficulty is with (*a*), (*b*). Whether the proposed method is feasible when the true continuity conditions (u, v, w continuous) are introduced requires further examination.

The following is an abstract of the communication made by Mr. Tucker (p. 311) entitled "The Brocardal Properties of some Associated Triangles":—

A_1AB_1, B_1BC_1, C_1CA_1 are drawn perpendicular to $A\Omega$, $B\Omega$, $C\Omega$, cutting the circumcircle in B', C', A' respectively; and, in like manner, A_2AC_2, B_2BA_2, C_2CA_2 perpendicular to $A\Omega'$, $B\Omega'$, $C\Omega'$, cutting the circle in C'', A'', B'' respectively. The equation to A_1B_1 is

$$\beta\cos\omega+\gamma\cos(A-\omega)=0, \qquad \text{(i.)}$$

and to A_2B_2 is

$$\alpha\cos\omega+\gamma\cos(B-\omega)=0. \qquad \text{(ii.)}$$

The points A_1, A_2 are given by

$$\cos(C-\omega)\cos(A-\omega),\quad -\cos\omega\cos(A-\omega),\quad \cos^2\omega, \qquad \text{(iii.)}$$

and by

$$\cos(A-\omega)\cos(B-\omega),\quad \cos^2\omega,\quad -\cos\omega\cos(A-\omega). \qquad \text{(iv.)}$$

We readily get

$$A_1B_1=c\operatorname{cosec}\omega=A_2B_2; \qquad \text{(v.)}$$

hence the triangles $A_1B_1C_1$ (or Δ_1) and $A_2B_2C_2$ (or Δ_2) are similar to ABC and are congruent to one another.

The points A', A'' are given by

$$-\cos(C-\omega)\cos(B+\omega),\quad \cos\omega\cos(B+\omega),\quad \cos\omega\cos(C-\omega), \qquad \text{(vi.)}$$

$$-\cos(B-\omega)\cos(C+\omega),\quad \cos\omega\cos(B-\omega),\quad \cos\omega\cos(B+\omega), \qquad \text{(vii.)}$$

and the triangles $A'B'C'$ (or Δ'), $A''B''C''$ (or Δ''), and ABC are congruent.

The circles (C_1), (C_2) round Δ_1, Δ_2 respectively, are given by

$$P.\Sigma a\beta\gamma+\cot\omega.\Sigma a\alpha\left[\Sigma\alpha\sin C\cos(B-\omega)\right]=0$$

and

$$P.\Sigma a\beta\gamma+\cot\omega.\Sigma a\alpha\left[\Sigma\alpha\sin B\cos(C-\omega)\right]=0,$$

where

$$P\equiv\operatorname{cosec}\omega.\Pi\sin A.$$

The circumcircle ABC can be readily shown to be the auxiliary circle of the Brocard ellipses of Δ_1, Δ_2.

The cyclic property (circumcentre O) of the six Brocard points of the five triangles and other properties are more elegantly derived from the theory of similar figures.

A referee writes: "We have as corresponding points of two similar figures

$$A,\ B,\ C;\quad A',\ B',\ C';\quad A_1,\ B_1,\ C_1;\ \dots;$$

$$A'',B'',C'';\quad A,\ B,\ C;\quad A_2,\ B_2,\ C_2;\ \dots;$$

the centre of similitude being O and the figures being congruent. Again, we may consider the three similar figures

$$A,\ B,\ C,\ \dots,\ K,\ \Omega,\ \Omega',\ O,\ \dots;$$

$$A_1, B_1, C_1, \dots, K_1,\ \Omega,\ \Omega_1,\ O_1.\ \dots;$$

$$A_2,\ B_2,\ C_2,\ \dots,\ K_2,\ \Omega_2,\ \Omega',\ O_2,\ \dots,$$

whose centres of similitude are O, Ω', Ω, and invariable points K, K_1, K_2 (the symmedian points); hence it follows that the symmedian points of $A_1B_1C_1$ and $A_2B_2C_2$ lie on the Brocard circle of ABC."

The accompanying notice of the late M. Hermite has been drawn up, at the request of the Council, by Mr. G. B. Mathews:—

Charles Hermite, whose death occurred on January 14th, 1901, was born at Dieuze, in Lorraine, December 24th, 1822. After school-days spent at Nancy and Paris, he entered the École Polytechnique in 1842, and soon gave evidence of his remarkable genius; for it was in 1843 that he wrote to Jacobi his well-known letter on the theory of Abelian functions, and this was followed in 1844 by another on the transformation of the elliptic functions. Adopting the profession of a teacher, his career was one of uninterrupted success; after holding several minor appointments he was elected in 1862 to a newly founded chair in the École Normale, and in 1869 to the professorship of higher analysis in the Sorbonne, which he held until 1897. Readers of his lithographed course will understand the enthusiasm with which his successor and former pupil, M. Picard, speaks of his charm as a lecturer; in judgment of selection and lucidity of exposition these lectures are unsurpassable, besides showing on every page the impress of an original mind. The festal celebration of Hermite's seventieth birthday showed in an impressive way the regard in which he was held by his pupils and fellow-workers alike; and we may hope that this was a bright day in a life which, like that of many other men of science, was, on the whole, retired and uneventful. It would be tedious to recount all the distinctions bestowed upon the great mathematician by learned societies; but it is proper to recall the fact that in 1871 (December 14th) he was elected foreign member of the London Mathematical Society, to the *Proceedings* of which he contributed three or four short papers.

Hermite was exclusively an analyst, and, above all perhaps, an arithmetician. He was an avowed disciple of Gauss, Jacobi, and Dirichlet; with the last two he frequently corresponded, and received from them an encouragement which must have done much to develop his powers. The brilliant discoveries of Jacobi naturally led Hermite to the study of elliptic and Abelian transcendents: his first two letters to Jacobi have already been referred to, and in subsequent years we have his researches on the elliptic modular functions, and, above all, the memoir *Sur quelques applications des fonctions elliptiques*, which contains, not only a discussion of Lamé's equation, which has become classical, but the extremely important theory of the decomposition of periodic functions into the sum of "simple elements," each with one (simple or multiple) pole. It may be observed that Hermite always adhered to the Jacobian elliptic and theta functions; partly, no doubt, because he had grown accustomed to them, but also, perhaps, because of their more obvious association with arithmetical theories. It is noticeable that the same thing may be said of Kronecker.

The invention of the calculus of invariants by Boole, Cayley, and Sylvester naturally attracted Hermite's attention, and he soon made substantial additions to the theory. To him is due the discovery of the first skew invariant, and the law of reciprocity which has been called after his name. Moreover, he showed the value of the new calculus by applying it to the transformation of elliptic functions, to the transcendental solution of the quintic, to the Tschirnhausen transformation, and to the separation of the roots of equations after the manner of Sturm.

It is in his arithmetical researches that Hermite's genius shows to greatest advantage. Here his familiarity with algebra on the one hand, and transcendent functions on the other, by converging to a focus, enable him to penetrate into depths otherwise inaccessible. His work on the reduction and classification of arithmetical forms is of the very highest importance, and involves a new and ingenious application of continuous parameters. His theory of forms with conjugate complex variables has shown itself capable of important developments, and he has made many beautiful applications of elliptic functions to arithmetic. One of his most famous achievements is the proof that e, the base of natural logarithms, is an essentially transcendental number.

Hermite had a large correspondence, and many of his most remarkable discoveries were communicated by letter to his friends. Göpel was induced to publish his classical memoir on Abelian functions by reading Hermite's first letter to Jacobi; had he not seen this, it is possible that he might have died without giving any of his work to the world.

A portrait of Hermite will be found in the *Annales de l'École Normale Supérieure*, t. XVIII. (1901), together with an excellent account of his scientific work by M. Émile Picard. It is to be hoped that a collected edition of Hermite's mathematical papers will be issued without unnecessary delay.

[It may be interesting to note that M. Hermite communicated the following Questions to the *Educational Times*: references are to the Volumes of the *Reprint*:—

Vol. VII., p. 37, 2254 (and Sylvester); p. 53, 2273. Vol. XXIX., p. 76, 5492. Vol. XLVI., p. 21, 8560; p. 50, 8510 (and solution); p. 63, 8588 (and solution); p. 94, 8633; p. 111, 8717. Vol. XLVII., p. 53, 8863 (and solution). Vol. XLVIII., p. 21, 9072. Vol. LI., p. 33, 9832; p. 49, 9930. Vol. LII., p. 63, 10125; p. 118, 10083. Vol. LIII., p. 127, 10155. Vol. LXVII., p. 91, 10267. Vol. LXV., p. 99, 12337.

R. T.]

INDEX.

INDEX OF PAPERS, &c.

[*The mark * indicates that the paper either has been printed* in extenso, *or an abstract of it given, in the "Proceedings."*]

Baker, H. F., M.A., F.R.S.
- (1) Remarks on Notation in Lie's Theory of Groups; and (2) on Schur's Determination of a Continuous Group of given structure, with remarks on Mr. Campbell's Paper (*cf.* pp. 285–294), p. 312.

Barnes, E. W., M.A.
- On the Zeroes of Bessel's Functions, p. 284.

Barwell, Miss M. E.
- On the Conformal Representation of Polygons on a Half Plane, p. 217.

Basset, A. B., M.A., F.R.S.
- On the Real Points of Inflexion of a Plane Curve, pp. 4, 217.

Bromwich, T. J. I'A., M.A.
- *Conformal Space Transformations, pp. 185–192.
- *Applications to Dynamics of some Algebraical Results, pp. 197–216.
- *Note on Stability of Motion, with an application to Hydrodynamics, pp. 325–342.

Burnside, Prof. W., M.A., F.R.S.
- *On Group Characteristics, pp. 146–162.
- *On some Properties of Groups of Odd Order, pp. 162–185.
- *On some Properties of Groups of Odd Order (Second Paper), pp. 257–268.

Campbell, J. E., M.A.
- *Proof of the Third Fundamental Theorem in Lie's Theory of Continuous Groups, pp. 285–294.

Carey, Prof. F. S., M.A.
- *On some Cases of the Solution of the Congruence $x^{p^n-1} \equiv 1$, mod p, pp. 294–310.

Carslaw, H. S., M.A.
- On Green's Function for a Circular Disc, p. 4.

Cunningham, Lt.-Col. A. J. C., R.E.
- *Factorisable Twin Binomials, pp. 361–380.

Dickson, L. E., Ph.D.
- *Concerning the Abelian and related Linear Groups, pp. 313–325.

Dixon, Prof. A C., M.A.
*Prime Functions on a Riemann Surface, pp. 10–26.

Dixon, A. L., M.A.
*An Addition Theorem for Hyperelliptic Theta Functions, pp. 274–283.

Elliott, Prof. E. B., M.A., F.R.S.
*The Syzygetic Theory of Orthogonal Binariants, pp. 226–257.

Glaisher, J. W. L., Sc.D., F.R.S.
*A general Congruence Theorem relating to the Bernoullian Function, pp. 27–56.
*On the Residues of Bernoullian Functions for a Prime Modulus, including as special cases the Residues of the Bernoullian, Eulerian, and *I*-Numbers, pp. 56–87.

Grace, J. H., M A.
*On a Class of Plane Curves, pp. 193–197.

Hudson, R. W. H. T., B.A.
*On Discriminants and Envelopes of Surfaces, pp. 269–274.
*A Geometrical Theory of Differential Equations of the First and Second Orders, pp. 380–403.

Kelvin, The Rt. Hon. Lord, G.C.V.O., F.R.S.
On the Transmission of Force through a Solid, p. 4.

Love, Prof. A. E. H., D.Sc., F.R.S.
On Streaming Motions past Cylindrical Boundaries, p. 284.

Mair, D. B., M.A.
Note on Curves Similar and Parallel to one another, p. 312.

Miller, G. A., Ph.D.
*In a Simple Group of an Odd Composite Order every System of Conjugate Operators or Sub-Groups includes more than Fifty, pp. 6–10.

Richmond, H. W., M.A.
*Note on the Inflexions of Curves with Double Points, pp. 218–226.

Stuart, T.
*The Distribution of Velocity and the Forms of the Stream Lines due to the Motion of an Ellipsoid in Fluid, Frictionless or Viscous, pp. 342–360.

Tucker, R., M.A.
*Notes on Isoscelians, pp. 87–90.
*Two In-triangles which are similar to the Pedal Triangle, pp. 91–97.
*The Brocardal Properties of some Associated Triangles, p. 211, 404.

Young, Alfred, M.A.
*On Quantitative Substitutional Analysis, pp. 97–146.

GENERAL INDEX.

Appendix (a) (1900-1901), 403-407.
Archiv der Math. Phys., 192.
Atti di Torino, 141.
Auditor, 1, 403.
Authors cited :—
  Andoyer, 227.
  Baker, H. F., 10, 24, 25, 26.
  Basset, 343, 352.
  Burnside, 6, 8, 165, 180, 262, 266.
  Burnside and Panton, 269, 270.
  Cayley, 274, 278, 281.
  Clebsch, 129.
  Elliott, 227.
  Euler, 364.
  Forsyth, 292, 390, 398.
  Greenhill, 335.
  Jordan, 6, 8, 179.
  Klein, 286.
  Klein-Sommerfeld, 208, 209, 334, 335.
  Kronecker, 204, 214, 216.
  Legendre, 364.
  Lie, 185, 186, 189, 285, 286.
  Lie-Scheffers, 384.
  Meyer, F., 221.
  Monge, 185.
  Muth, 204.
  Poincaré, 328.
  Riemann, 192.
  Routh, R., Dyn., 198 ; Stability, 331, 332, 336.
  Salmon, H., Alg., 273 ; H.P.C., 221 ; S.G., 275.
  Serret, 294.
  Thomson and Tait, 197, 213.
  Weber, 146.
Basset, A. B., 331.
Beltrami, 1, 185.
Berliner Monatsber., 204, 205, 214, 216.
——— Sitzungsber., 146, 170.
Borchardt, 312.
Brill, 218 &c.
Bromwich, 201, 202, 205, 209, 215, 337.
Burnside, W., 7, 100, 149 &c., 165, 180, 257, 268.
Camb. Phil. Soc. Proc., 331, 335.
——————— Trans., 285.
Campbell, J. E., 186, 290.
Capelli, 99, 119, 139.
Caporali, 219.
Cayley, 381, 382.
Clebsch, 339, 352.
Clerk Maxwell, 185.
Clifford, 193.
Close, F., 1.
Comptes Rendus, 166, 193, 216, 336.
Council, Election of, 3.
Crelle, 204, 336, 352, 390.
Cunningham, A. J. C., 361, 364, 366, 369, 372, 378.
Darboux, 185, 192.
Definitions :—
  Bin-Aurifeuillians, 366.
  Forms (Binomial, Twin, and Non-equivalent), 361.
  Group-characteristics, A set of, 147.
  $+I_A$, $-I_A$, 87.
  Prime and Factor Functions, and Accidental Factors, 11.
  Quasi- and Anti-quasi-conformals, 370.
  Sets, Inverse and Self-Inverse, 148, 154.
  Stability, 326
  Trin-Aurifeuillians, 369.
  $\Omega(r)$, 32.
Dickson, L. E., 313, 319.
Dixon, A. C., 10, 14.
Ecole Polytech., Journal de l', 185.
Edwardes, D., 342.
Elliott, E. B., 212.
Encyc. Brit. (Hydromechanics), 341.
Errata, 14 (note), 403.
Exchanges, 1, 2 (and as under "Library, Presents to").
Fawcett, Miss, 340.
Fine, H. B., 387, 392.
Forsyth, 270, 281.
Frobenius, 146 &c., 170.
Gallop, 1, 403.
Gentry, Miss R., 219.
Gerbaldi, 219.
Glaisher, 27 &c.
Göttingen Nachrichten, 185.
Gordan, 99, 141.
Goupillière, J. N. H. de, 185.
Goursat, 396.
Greenhill, 334, 335, 341.
Groups, Imprimitive, 180-184.
Hamburger, 390.
Henrici, 271, 381, 400.
Herman, 352.
Hermite, 311, 405.
Hill, M. J. M., 271, 382, 383, 390.
Hobson, 4, 310.
Index (to Vols. I.-XXX.), 3.
Jenkins, M., 3.
Jordan, 216.

Kelvin, Lord, 3, 4.
Kempe, 1, 231.
Klein, 10, 24, 25, 208, 218, 286, 325, 332, 342.
Kneser, 336.
Kötter, 218.
Larmor, J., 311, 335.
Levi-Civita, 331.
Liapunoff, 336.
Library, Presents to, 4, 217, 284, 312.
Lincei, R. Accad. dei, 185, 218.
Liouville, 183, 186, 216, 336.
Loewy, 166.
Love, A. E. H., 326 &c.
Lucas, E., 378.
MacMahon, 226, 231.
Matematica, Ann. di, 219, 331.
Mathematical Soc., Bulletin of American, 208, 334, 341.
——————— Trans. of American, 193, 313.
——————— Proc. of London, 6, 7, 9, 10, 14, 27, 28, 48, 52, 56, 66, 72, 74, 93, 98, 99, 149, 152, 154, 160, 163, 166, 171, 179, 185, 201, 202, 205, 220, 231, 266, 268, 271, 290, 314, 334, 361, 362, 364, 366, 369, 372, 378, 381, 382, 389, 390, 400.
Mathematics, Messenger of, 31, 53, 54, 58, 67, 70, 73, 75, 186, 381, 382, 383.
—————— Amer. Jour. of, 201, 215, 335, 341, 387, 392, 396.
—————— Quart. Jour. of, 8, 28, 31, 36, 48, 49, 52, 53, 60, 65, 76, 77, 209, 220, 221, 314, 319, 340, 341, 342, 352.
Mathématiques, Journal de, 185.
Mathematische Annalen, 10, 24, 25, 119, 166, 185, 218, 219, 221, 259, 339, 382.
Mathews, G. B., 405.
Meeting, Annual, 1-5.
———— General (*cf.* Papers read).
Members, Admission of, 284.
———— Election of, 217, 284.
———— Number of, 3.
———— Present at Meetings, 1, 217, 284, 310.
———— List of (1865-1899), 3.
Michell, J. H., 403.
Miller, G. A., 6, 8, 9, 163, 178, 179.
Moore, E. H., 166.
Morley, F., 193.
Napoli, Rendic. dell' Acc. delle Scienze di, 219.
Nöther, 25.
Oberbeck, 342.
Obituary, 1, 310, 311, 405.
Painlevé, 336.
Palermo, Rend. del Circ. Mat. di, 219.
Papers read, 4, 217, 284, 310.
Peano, 99, 141.
Petrovitch, 382.
Phil. Trans., 279, 281.
Poincaré, 285.
Queen's death, President's remarks on, 310.
Referees, Obligations to, 93 (footnote), 97, 100, 222, 257, 326, 405.
Report, Auditor's, 403.
——— Secretaries', 1-3.
——— Treasurer's, 1, 403.
Residues, Tables of, 302-310.
Richmond, H. W., 221.
Roberts, W. R. W., 220.
Royal Soc. of Edin., Proc. of, 186.
————————— Trans. of, 186.
Schottky, 25.
Schur, 285.
Scrutineers, 3.
Segre, 218, 219.
Serret, Paul, 193.
Stickelberger, 204.
Sheppard, 1.
Taber, 205.
Tait, 186.
Taylor, W. W., 3.
Thanks, Vote of, Lord Kelvin, 4.
Tucker, R., 93, 311.
Types of Groups, Table of, 323.
Walker, J. J., 1.
Weierstrass, 205, 214.
Whittaker, E. T., 197.
Work, Secretaries' extra, 3.
Young, Alfred, 98, 99, 141.
Zeuthen, 219.

Printed by C. F. Hodgson & Son, 2 Newton Street, High Holborn, W.C.

VOLUMES ALREADY ISSUED.

Vol.	**I.**	**(from January 1865 to November 1866)**		**10*s*.**
,,	**II.**	**(from November 1866 to November 1869)**		**16*s*.**
,,	**III.**	**(from November 1869 to November 1871)**		**20*s*.**
,,	**IV.**	**(from November 1871 to November 1873)**		**31*s*. 6*d*.**
,,	**V.**	**(from November 1873 to November 1874)**		**15*s*.**
,,	**VI.**	**(from November 1874 to November 1875)**		**21*s*.**
,,	**VII.**	**(from November 1875 to November 1876)**		**21*s*.**
,,	**VIII.**	**(from November 1876 to November 1877)**		**21*s*.**
,,	**IX.**	**(from November 1877 to November 1878)**		**21*s*.**
,,	**X.**	**(from November 1878 to November 1879)**		**18*s*.**
,,	**XI.**	**(from November 1879 to November 1880)**		**12*s*. 6*d*.**
,,	**XII.**	**(from November 1880 to November 1881)**		**16*s*.**
,,	**XIII.**	**(from November 1881 to November 1882)**		**18*s*.**
,,	**XIV.**	**(from November 1882 to November 1883)**		**20*s*.**
,,	**XV.**	**(from November 1883 to November 1884)**		**20*s*.**
,,	**XVI.**	**(from November 1884 to November 1885)**		**20*s*.**
,,	**XVII.**	**(from November 1885 to November 1886)**		**25*s*.**
,,	**XVIII.**	**(from November 1886 to November 1887)**		**25*s*.**
,,	**XIX.**	**(from November 1887 to November 1888)**		**30*s*.**
,,	**XX.**	**(from November 1888 to November 1889)**		**25*s*.**
,,	**XXI.**	**(from November 1889 to November 1890)**		**25*s*.**
,,	**XXII.**	**(from November 1890 to November 1891)**		**27*s*. 6*d*.**
,,	**XXIII.**	**(from November 1891 to November 1892)**		**20*s*.**
,,	**XXIV.**	**(from November 1892 to November 1893)**		**22*s*.**
,,	**XXV.**	**(from November 1893 to November 1894)**		**22*s*.**
,,	**XXVI.**	**(from November 1894 to November 1895)**		**30*s*.**
,,	**XXVII.**	**(from November 1895 to November 1896)**		**35*s*.**
,,	**XXVIII.**	**(from November 1896 to November 1897)**		**32*s*. 6*d*.**
,,	**XXIX.**	**(from November 1897 to November 1898)**	Part I.	**20*s*.**
			Part II.	**20*s*.**
,,	**XXX.**	**(from November 1898 to March 1899)**		**20*s*.**
,,	**XXXI.**	**(from April 1899 to December 1899)**		**20*s*.**
,,	**XXXII.**	**(from January 1900 to June 1900)**		**20*s*.**
,,	**XXXIII.**	**(from November 1900 to February 1901)**		**20*s*.**